

IBM Director 4.20



# Installation and Configuration Guide



IBM Director 4.20



# Installation and Configuration Guide

**Note:** Before using this information and the product it supports, read the general information in Appendix C, “Notices,” on page 247.



**Third Edition (July 2004)**

**© Copyright International Business Machines Corporation 2004. All rights reserved.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

---

# Contents

<b>Figures</b> . . . . .	vii
<b>Tables</b> . . . . .	xi
<b>About this book</b> . . . . .	xiii
How this book is organized . . . . .	xiii
Notices that are used in this book . . . . .	xiv
IBM Director documentation . . . . .	xiv
IBM Director resources on the World Wide Web . . . . .	xv

---

## Part 1. Overview of IBM Director . . . . . 1

<b>Chapter 1. Introducing IBM Director</b> . . . . .	3
IBM Director environment . . . . .	3
IBM Director components . . . . .	4
IBM Director Agent features . . . . .	6
IBM Director extensions . . . . .	7
Licensing . . . . .	11
Upgrading from previous releases of IBM Director . . . . .	11
<b>Chapter 2. Requirements for installing IBM Director</b> . . . . .	13
Hardware requirements . . . . .	13
Supported operating systems . . . . .	14
Network requirements . . . . .	18
Supported Web browsers for Web-based Access . . . . .	20
Supported database applications . . . . .	20
<b>Chapter 3. Planning your IBM Director installation</b> . . . . .	21
General planning considerations . . . . .	21
Managing service processors . . . . .	22
Setting up a BladeCenter deployment infrastructure . . . . .	27
Preparing the IBM Director database . . . . .	28
IBM Director security . . . . .	32

---

## Part 2. Installing IBM Director . . . . . 37

<b>Chapter 4. Installing IBM Director Server</b> . . . . .	39
Preparing to install IBM Director Server on an xSeries server . . . . .	39
Installing IBM Director Server on i5/OS . . . . .	41
Installing IBM Director Server on Linux . . . . .	41
Installing IBM Director Server on Windows . . . . .	44
<b>Chapter 5. Installing IBM Director Console</b> . . . . .	57
Installing IBM Director Console on Linux . . . . .	57
Installing IBM Director Console on Windows . . . . .	58
<b>Chapter 6. Installing IBM Director Agent</b> . . . . .	63
Preparing to install IBM Director Agent on an xSeries server . . . . .	63
Installing IBM Director Agent on AIX . . . . .	65
Installing IBM Director Agent on i5/OS . . . . .	66
Installing IBM Director Agent on Linux . . . . .	66
Installing IBM Director Agent on NetWare . . . . .	68

Installing IBM Director Agent on Windows (32-bit) . . . . .	71
Installing IBM Director Agent on Windows (64-bit) . . . . .	78

---

**Part 3. Configuring IBM Director . . . . . 85**

<b>Chapter 7. Configuring IBM Director . . . . .</b>	<b>87</b>
Starting IBM Director Console . . . . .	87
Using the Event Action Plan wizard . . . . .	88
Discovering managed systems, devices, and objects . . . . .	93
Authorizing IBM Director users . . . . .	97
Configuring security settings . . . . .	103
Configuring software distribution . . . . .	106
 <b>Chapter 8. Configuring an IBM BladeCenter chassis . . . . .</b>	 <b>113</b>
Discovering a BladeCenter chassis . . . . .	113
Using the BladeCenter Deployment wizard . . . . .	116
 <b>Chapter 9. Installing IBM Director extensions . . . . .</b>	 <b>131</b>
Completing the Rack Manager installation on the management server . . . . .	131
Installing Software Distribution (Premium Edition). . . . .	132
Preparing to install the Server Plus Pack extensions on managed systems . . . . .	134
Installing the Server Plus Pack extensions on managed systems . . . . .	134

---

**Part 4. Upgrading IBM Director . . . . . 145**

<b>Chapter 10. Upgrading IBM Director Server . . . . .</b>	<b>147</b>
Preparing to upgrade IBM Director Server on an xSeries server . . . . .	147
Upgrading IBM Director Server on Linux . . . . .	150
Upgrading IBM Director Server on Windows. . . . .	152
 <b>Chapter 11. Upgrading IBM Director Console . . . . .</b>	 <b>161</b>
Upgrading IBM Director Console on Linux . . . . .	161
Upgrading IBM Director Console on Windows . . . . .	163
 <b>Chapter 12. Upgrading IBM Director Agent . . . . .</b>	 <b>169</b>
Preparing to upgrade IBM Director Agent on an xSeries server. . . . .	169
Upgrading IBM Director Agent using standard installation procedures . . . . .	172
Upgrading IBM Director Agent using the Software Distribution task . . . . .	189

---

**Part 5. Maintenance and problem solving . . . . . 195**

<b>Chapter 13. Modifying and uninstalling IBM Director . . . . .</b>	<b>197</b>
Modifying an IBM Director installation . . . . .	197
Uninstalling IBM Director. . . . .	204
 <b>Chapter 14. Solving IBM Director problems . . . . .</b>	 <b>209</b>
Installation, upgrades, and uninstallation . . . . .	209
IBM Director Server. . . . .	211
IBM Director Console . . . . .	215
IBM Director Agent . . . . .	219
Managed systems running Windows . . . . .	220
IBM Director tasks . . . . .	221
Software Distribution . . . . .	224
Web-based Access . . . . .	226
Systems running double-byte character set languages . . . . .	227

<b>Chapter 15. Getting help and technical assistance</b> . . . . .	229
Before you call . . . . .	229
Using the documentation. . . . .	229
Getting help and information from the World Wide Web . . . . .	230
Software service and support . . . . .	230

---

**Part 6. Appendixes** . . . . . 231

<b>Appendix A. IBM Director Agent — IBM Director Server security</b> . . . . .	233
How authentication works . . . . .	233
Securing managed systems. . . . .	235
Changing access or security states . . . . .	237
Key management . . . . .	238
<b>Appendix B. Terminology summary and abbreviation list</b> . . . . .	241
IBM Director terminology summary . . . . .	241
Abbreviations . . . . .	241
<b>Appendix C. Notices</b> . . . . .	247
Edition notice . . . . .	248
Trademarks. . . . .	248
<b>Glossary</b> . . . . .	249
<b>Index</b> . . . . .	259



# Figures

1. Hardware in an IBM Director environment . . . . .	4
2. Software in an IBM Director environment . . . . .	5
3. Example of a BladeCenter deployment network . . . . .	27
4. Installing IBM Director Server on Windows: “Server Plus Pack” window . . . . .	45
5. Installing IBM Director Server on Windows: “Feature and installation directory selection” window . . . . .	45
6. Installing IBM Director Server on Windows: “Features and installation directory selection” window . . . . .	46
7. Installing IBM Director Server on Windows: Installing the Server Plus Pack . . . . .	47
8. Installing IBM Director Server on Windows: “IBM Director service account information” window . . . . .	48
9. Installing IBM Director Server on Windows: “Encryption settings” window . . . . .	49
10. Installing IBM Director Server on Windows: “Software-distribution settings” window . . . . .	49
11. Installing IBM Director Server on Windows: “Web-based Access information” window . . . . .	50
12. Installing IBM Director Server on Windows: “Network driver configuration” window . . . . .	51
13. Installing IBM Director Server: “IBM Director database configuration” window . . . . .	52
14. Installing IBM Director Server: “IBM Director DB2 Universal Database configuration” window . . . . .	53
15. Installing IBM Director Server: “IBM Director DB2 Universal Database configuration” window . . . . .	54
16. Installing IBM Director Server: “IBM Director Microsoft SQL Server database configuration” window . . . . .	54
17. Installing IBM Director Server: “IBM Director Oracle database configuration” window . . . . .	55
18. Installing IBM Director Server: “IBM Director Oracle database configuration” window . . . . .	56
19. Installing IBM Director Console: “Server Plus Pack” window . . . . .	59
20. Installing IBM Director Console: “Feature and destination directory selection” window . . . . .	59
21. Installing IBM Director Console: Installing ServeRAID Manager . . . . .	60
22. Installing IBM Director Console: Installing the Server Plus Pack . . . . .	61
23. Installing IBM Director Agent on NetWare: “Choose destination location” window . . . . .	69
24. Installing IBM Director Agent on NetWare: “Select Components” window . . . . .	69
25. Installing IBM Director Agent on NetWare: “InstallShield Wizard complete” window . . . . .	70
26. Installing IBM Director Agent on Windows: “Feature and installation directory selection” window . . . . .	72
27. Installing IBM Director Agent on Windows: “Feature and installation directory selection” window . . . . .	73
28. Installing IBM Director Agent on Windows: “Security settings” window . . . . .	73
29. Installing IBM Director Agent on Windows: “Software Distribution settings” window . . . . .	74
30. Installing IBM Director Agent on Windows: “Web-based Access information” window . . . . .	75
31. Installing IBM Director Agent on Windows: “Network driver configuration” window . . . . .	76
32. Installing IBM Director Agent on Windows: “Feature and installation directory selection” window . . . . .	79
33. Installing IBM Director Agent on Windows: “Security settings” window . . . . .	80
34. Installing IBM Director Agent on Windows: “Software Distribution settings” window . . . . .	80
35. Installing IBM Director Agent on Windows: “Network driver configuration” window . . . . .	81
36. “IBM Director Login” window . . . . .	87
37. IBM Director Console . . . . .	88
38. Event Action Plan wizard: “Welcome to the Event Action Plan wizard” window . . . . .	89
39. Event Action Plan wizard: “Select the event filters” window . . . . .	89
40. Event Action Plan wizard: “Select the notification” window . . . . .	90
41. Event Action Plan wizard: “Apply the event action plan” window . . . . .	92
42. Event Action Plan wizard: “Discover all systems and devices” window . . . . .	92
43. Event Action Plan wizard: “Review your selection summary” window . . . . .	93
44. “Discovery Preferences” window . . . . .	95
45. “Add Management Processors” window . . . . .	96
46. IBM Director Console: Group Contents pane . . . . .	97
47. “User Administration” window . . . . .	98
48. “User Defaults Editor” window . . . . .	98
49. “User Administration” window . . . . .	99
50. “User Editor” window: “User Properties” page . . . . .	100
51. “User Editor” window: “Privileges” page . . . . .	100
52. “User Editor” window: “Group Access” page . . . . .	101

53. “User Editor” window: “Task Access” page . . . . .	102
54. IBM Director Console: “Add Share Name” window . . . . .	108
55. IBM Director Console: “Software Distribution” page . . . . .	109
56. IBM Director Console: “Managed System Distribution Preferences” window . . . . .	110
57. IBM Director Console: “Add Share Name” window . . . . .	111
58. IBM Director Console: Group Contents pane . . . . .	114
59. “Add BladeCenter Chassis” window . . . . .	115
60. “Management Module Network Interfaces” window . . . . .	116
61. BladeCenter Deployment wizard: “Welcome to the BladeCenter Deployment wizard” window . . . . .	119
62. BladeCenter Deployment wizard: “Login to the BladeCenter management module” window . . . . .	120
63. BladeCenter Deployment wizard: “Change the user name and password for the management module” window. . . . .	121
64. BladeCenter Deployment wizard: “Configure the management module properties” window . . . . .	122
65. BladeCenter Deployment wizard: “Configure the management module protocols” window . . . . .	123
66. BladeCenter Deployment wizard: “Configure the IP addresses” window . . . . .	124
67. BladeCenter Deployment wizard: “Change the user name and password for the switch modules” window . . . . .	125
68. BladeCenter Deployment wizard: “Configure the switch module” window . . . . .	126
69. BladeCenter Deployment wizard: “Deploy operating systems to the blade servers” window . . . . .	127
70. BladeCenter Deployment wizard: “Configure the deployment policies” window . . . . .	128
71. BladeCenter Deployment wizard: “Setup summary” window. . . . .	129
72. IBM Director Console Tasks pane: BladeCenter Deployment wizard profile . . . . .	130
73. Installing Capacity Manager on NetWare: “Choose Destination Location” window. . . . .	136
74. Installing Capacity Manager on NetWare: “Start Copying Files” window . . . . .	137
75. Creating a software package: “Software Distribution Manager” window (Standard Edition) . . . . .	138
76. Creating a software package: “Software Distribution Manager” window (Premium Edition) . . . . .	139
77. Creating a software package: “Director Update Assistant” window . . . . .	139
78. Creating a software package: “IBM Update Package/Root Directory Location” window . . . . .	140
79. Creating a software package: “IBM Update Package/Root Directory Location” window . . . . .	140
80. Creating software packages: “Director Update Assistant” window. . . . .	141
81. Creating software packages: “Director Update Assistant” window. . . . .	141
82. All Software Distribution Packages: IBM Director Server Plus Pack . . . . .	142
83. Scheduling the installation of a software package: “New Scheduled Job” window. . . . .	143
84. Upgrading IBM Director Server on Windows: “Server Plus Pack” window. . . . .	153
85. Upgrading IBM Director Server on Windows: “Feature and installation directory selection” window . . . . .	153
86. Upgrading IBM Director Server on Windows: “Feature and installation directory selection” window . . . . .	154
87. Upgrading IBM Director Server on Windows: Installing the Server Plus Pack . . . . .	155
88. Upgrading IBM Director Server on Windows: “IBM Director service account information” window . . . . .	156
89. Installing IBM Director Server on Windows: “Encryption settings” window. . . . .	157
90. Upgrading IBM Director Server on Windows: “Software-distribution settings” window . . . . .	157
91. Upgrading IBM Director Server on Windows: “Web-based Access information” window. . . . .	158
92. Upgrading IBM Director Server on Windows: “Network driver configuration” window. . . . .	159
93. Upgrading IBM Director Console: “Server Plus Pack” window . . . . .	164
94. Upgrading IBM Director Console: “Feature and destination directory selection” window . . . . .	164
95. Upgrading IBM Director Console: Installing ServeRAID Manager. . . . .	165
96. Upgrading IBM Director Console: Installing the Server Plus Pack . . . . .	166
97. Upgrading IBM Director Agent on NetWare: “Select Components” window . . . . .	175
98. Upgrading IBM Director Agent on Windows: “Feature and installation directory selection” window . . . . .	176
99. Upgrading IBM Director Agent on Windows: “Feature and installation directory selection” window . . . . .	177
100. Upgrading IBM Director Agent on Windows: “Security settings” window . . . . .	178
101. Upgrading IBM Director Agent on Windows: “Software Distribution settings” window. . . . .	179
102. Upgrading IBM Director Agent on Windows: “Web-based Access information” window . . . . .	180
103. Upgrading IBM Director Agent on Windows: “Network driver configuration” window . . . . .	181
104. Installing IBM Director Agent on Windows: “Feature and installation directory selection” window . . . . .	184
105. Installing IBM Director Agent on Windows: “Security settings” window . . . . .	185
106. Upgrading IBM Director Agent on Windows: “Software Distribution settings” window. . . . .	186

107. Installing IBM Director Agent on Windows: “Network driver configuration” window . . . . .	187
108. Creating a software package: “Software Distribution Manager” window (Standard Edition)	190
109. Creating a software package: “Software Distribution Manager” window (Premium Edition)	190
110. Creating a software package: “Director Update Assistant” window . . . . .	191
111. Creating a software package: “IBM Update Package/Root Directory Location” window . . . . .	191
112. Creating a software package: “IBM Update Package/Root Directory Location” window . . . . .	192
113. Creating a software package: “Director Update Assistant” window . . . . .	192
114. Creating software packages: “Director Update Assistant” window. . . . .	193
115. All Software Distribution Packages: IBM Director Agent Upgrade . . . . .	193
116. Scheduling the installation of a software package: “New Scheduled Job” window. . . . .	194
117. Modifying IBM Director Agent on NetWare: “Choose destination location” window . . . . .	202
118. Modifying IBM Director Agent on NetWare: “Select Components” window . . . . .	202
119. “Program Maintenance” window . . . . .	204
120. “Request Access to Systems” window. . . . .	237



---

## Tables

1. Intel-compatible systems and @server JS20 blade servers: Minimum hardware requirements	13
2. iSeries servers: Minimum hardware requirements . . . . .	14
3. iSeries servers: Required products and options. . . . .	14
4. Supported operating systems for Server Plus Pack extensions installed on managed systems	17
5. Supported versions of network protocols . . . . .	18
6. Types of data transmission and supported network protocols. . . . .	18
7. Ports used by IBM Director . . . . .	19
8. Database applications supported by IBM Director . . . . .	20
9. In-band communication between service processors and IBM Director Server . . . . .	23
10. IBM Director Agent features that handle in-band alerts . . . . .	24
11. Gateway service processors and communication with service processors on an ASM interconnect network . . . . .	25
12. Out-of-band alerting pathways . . . . .	26
13. Out-of-band alert-forwarding strategies . . . . .	26
14. IBM Director user groups . . . . .	33
15. Encryption state and data transmitted between IBM Director Server and IBM Director Agent	35
16. Installing IBM Director Server: IBM LM78 and SMBus device drivers for Linux . . . . .	39
17. Installing IBM Director Server: Source files for the LM78 and SMBus device drivers . . . . .	40
18. Installing IBM Director Agent: IBM LM78 and SMBus device drivers for Linux . . . . .	63
19. Installing IBM Director Agent: Source files for the LM78 and SMBus device drivers . . . . .	64
20. IBM Active PCI Software necessary to run Active PCI Manager . . . . .	134
21. Network adapter device drivers necessary to run the Fault Tolerant Management Interface	134
22. Upgrading IBM Director Server: IBM LM78 and SMBus device drivers for Linux . . . . .	148
23. Upgrading IBM Director Server: Source files for the LM78 and SMBus device drivers . . . . .	149
24. Upgrading IBM Director Agent: IBM LM78 and SMBus device drivers for Linux . . . . .	170
25. Upgrading IBM Director Agent: Source files for the LM78 and SMBus device drivers . . . . .	171
26. dirunins parameters . . . . .	207
27. Installation problems . . . . .	209
28. Upgrade problems . . . . .	210
29. Uninstallation problems . . . . .	211
30. IBM Director Server problems. . . . .	211
31. IBM Director Console problems . . . . .	215
32. IBM Director Agent problems . . . . .	219
33. Managed systems running Windows problems . . . . .	220
34. IBM Director task problems . . . . .	221
35. Software Distribution problems . . . . .	224
36. Web-based Access problems . . . . .	226
37. Systems running double-byte character set languages problems . . . . .	227
38. Initial security state of IBM Director Agent . . . . .	234
39. Abbreviations used in IBM Director. . . . .	241



---

## About this book

This book provides information about installing and configuring IBM® Director 4.20. In addition to presenting an overview of IBM Director and its requirements, it covers the following topics:

- Planning an IBM Director environment
- Installing IBM Director and IBM Director extensions
- Upgrading from IBM Director 3.1 or later to IBM Director 4.20
- Configuring IBM Director

It also includes information about IBM Director security and solving problems you might encounter with IBM Director.

---

## How this book is organized

Chapter 1, “Introducing IBM Director,” on page 3 contains an overview of IBM Director, including its components, features, and extensions.

Chapter 2, “Requirements for installing IBM Director,” on page 13 contains basic information about IBM Director. This includes system and network requirements, supported operating systems and database applications, information about the IBM user accounts, and an overview of IBM Director security features.

Chapter 3, “Planning your IBM Director installation,” on page 21 contains information about planning your IBM Director environment. It also includes information about working with service processors, setting up a BladeCenter™ deployment infrastructure, and preparing a database for use with IBM Director.

Chapter 4, “Installing IBM Director Server,” on page 39 contains instructions for installing IBM Director Server.

Chapter 5, “Installing IBM Director Console,” on page 57 contains instructions for installing IBM Director Console.

Chapter 6, “Installing IBM Director Agent,” on page 63 contains instructions for installing IBM Director Agent.

Chapter 7, “Configuring IBM Director,” on page 87 contains information about starting IBM Director Console, running the Event Action Plan wizard, setting discovery preferences and creating management processor objects, authorizing IBM Director users, configuring security settings, and preparing to use software distribution.

Chapter 8, “Configuring an IBM BladeCenter chassis,” on page 113 contains information about discovering the BladeCenter chassis and running the BladeCenter Deployment wizard.

Chapter 9, “Installing IBM Director extensions,” on page 131 contains instructions for completing the Rack Manager installation on the management server, installing IBM Director Software Distribution (Premium Edition), and installing the IBM Director Server Plus Pack extensions on managed systems.

Chapter 10, “Upgrading IBM Director Server,” on page 147 contains instructions for upgrading IBM Director Server.

Chapter 11, “Upgrading IBM Director Console,” on page 161 contains instructions for upgrading IBM Director Console.

Chapter 12, “Upgrading IBM Director Agent,” on page 169 contains instructions for upgrading IBM Director Agent.

Chapter 13, “Modifying and uninstalling IBM Director,” on page 197 contains information about modifying and uninstalling IBM Director.

Chapter 14, “Solving IBM Director problems,” on page 209 lists solutions to problems that you might encounter with IBM Director.

Chapter 15, “Getting help and technical assistance,” on page 229 contains information about accessing IBM Support Web sites for help and technical assistance.

Appendix A, “IBM Director Agent — IBM Director Server security,” on page 233 contains information about IBM Director Agent — IBM Director Server security. It includes an overview of authentication, procedures for securing managed systems, and information about key management.

Appendix B, “Terminology summary and abbreviation list,” on page 241 contains a summary of IBM Director terminology and a list of abbreviations used in IBM Director publications.

Appendix C, “Notices,” on page 247 contains product notices and trademarks.

The “Glossary” provides definitions for the terms used that are used in IBM Director documentation.

---

## Notices that are used in this book

This book contains the following notices designed to highlight key information:

- **Notes:** These notices provide important tips, guidance, or advice.
- **Important:** These notices provide information or advice that might help you avoid inconvenient or difficult situations.
- **Attention:** These notices indicate possible damage to programs, devices, or data. An attention notice is placed just before the instruction or situation in which damage could occur.

---

## IBM Director documentation

The following documents are available in Portable Document Format (PDF) from the IBM Director 4.20 Web site at

<http://www.ibm.com/pc/support/site.wss/document.do?Indocid=MIGR-55606>:

- *IBM Director 4.20 Installation and Configuration Guide* Third Edition, July 2004 (dir4.20\_docs\_install.pdf)
- *IBM Director 4.20 Systems Management Guide* Third Edition, July 2004 (dir4.20\_docs\_sysmgt.pdf)
- *IBM Director 4.1 Events Reference* (dir41\_events.pdf)
- *IBM Director 4.20 Upward Integration Modules Installation Guide* Second Edition, July 2004 (dir4.20\_docs\_uim.pdf)

For planning purposes, the following IBM @server<sup>®</sup> and xSeries<sup>®</sup> documents might be of interest:

- *IBM @server BladeCenter Type 8677 Planning and Installation Guide*
- *Remote Supervisor Adapter, User's Guide*
- *Remote Supervisor Adapter, Installation Guide*
- *Remote Supervisor Adapter II, User's Guide*
- *Remote Supervisor Adapter II, Installation Guide*
- *IBM Management Processor Command-Line Interface Version 2.0 User's Guide*

You can obtain these documents from the IBM Support Web site at <http://www.ibm.com/pc/support/>.

In addition, the following IBM Redbooks<sup>™</sup> documents might be of interest:

- *Creating a Report of the Tables in the IBM Director 4.1 Database (TIPS0185)*
- *IBM Director Security (REDP-0417-00)*
- *IBM @server BladeCenter Systems Management with IBM Director V4.1 and Remote Deployment Manager V4.1 (REDP-3776-00)*
- *Implementing Systems Management Solutions using IBM Director (SG24-6188)*
- *Integrating IBM Director with Enterprise Management Solutions (SG24-5388)*
- *Managing IBM TotalStorage NAS with IBM Director (SG24-6830)*
- *Monitoring Redundant Uninterruptible Power Supplies Using IBM Director (REDP-3827-00)*

You can download these documents from the IBM Redbooks Web site at <http://www.ibm.com/redbooks/>. You also might want to search this Web site for documents that focus on specific IBM hardware; such documents often contain systems-management material.

**Note:** Be sure to note the date of publication and to determine the level of IBM Director software to which the Redbooks publication refers.

---

## IBM Director resources on the World Wide Web

The following Web pages provide resources for understanding, using, and troubleshooting IBM Director and systems-management tools.

### IBM Director 4.20

<http://www.ibm.com/pc/support/site.wss/document.do?Indocid=MIGR-55606>

You can download the following IBM Director 4.20 code and information from this Web page:

- CD image
- Documentation
- IBM LM78 and system management bus (SMBus) device drivers for Linux<sup>®</sup>
- Readme files
- Extensible Markup Language (XML) files for use with the Software Distribution task

Check this Web page regularly for updated readme files and documentation.

**IBM Director Agent page**

[http://www.ibm.com/servers/eserver/xseries/systems\\_management/sys\\_migration/ibmdiragent.html](http://www.ibm.com/servers/eserver/xseries/systems_management/sys_migration/ibmdiragent.html)

You can download the IBM Director Hardware and Software Compatibility document from this Web page. This document lists supported @server and xSeries systems, as well as all supported operating systems. It is updated every 6 to 8 weeks.

**IBM @server Information Center**

<http://www.ibm.com/servers/library/infocenter>

This Web page provides information about the IBM Virtualization Engine™ and IBM Director Multiplatform.

**IBM ServerProven page**

<http://www.ibm.com/pc/us/compat/index.html>

The ServerProven® Web page provides information about xSeries, BladeCenter, and IntelliStation® hardware compatibility with IBM Director.

**IBM Support page**

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

This is the IBM Support Web site for IBM hardware and systems-management software. For systems-management software support, click **Systems management**.

**IBM Systems Management Software: Download/Electronic Support page**

[http://www.ibm.com/pc/us/eserver/xseries/systems\\_management/dwnl.html](http://www.ibm.com/pc/us/eserver/xseries/systems_management/dwnl.html)

Use this Web page to download IBM systems-management software, including IBM Director. Check this Web page regularly for new IBM Director releases and updates.

**IBM xSeries Systems Management page**

[http://www.ibm.com/pc/ww/eserver/xseries/systems\\_management/index.html](http://www.ibm.com/pc/ww/eserver/xseries/systems_management/index.html)

This Web page presents an overview of IBM systems management and IBM Director. It also contains links to Web pages for IBM Director extensions including Remote Deployment Manager, Scalable Systems Manager, Server Plus Pack, and Software Distribution (Premium Edition).

---

## Part 1. Overview of IBM Director



---

## Chapter 1. Introducing IBM Director

IBM Director is a comprehensive systems-management solution. Based on industry standards, it can be used with most Intel<sup>®</sup>-microprocessor-based systems and certain IBM @server iSeries<sup>™</sup> and pSeries<sup>®</sup> servers.

A powerful suite of tools and utilities, IBM Director automates many of the processes that are required to manage systems proactively, including capacity planning, asset tracking, preventive maintenance, diagnostic monitoring, troubleshooting, and more. It has a graphical user interface that provides easy access to both local and remote systems.

IBM Director can be used in environments with multiple operating systems (heterogeneous environments) and integrated with robust workgroup and enterprise management software from IBM (such as Tivoli<sup>®</sup> software), Computer Associates, Hewlett-Packard, Microsoft<sup>®</sup>, NetIQ, and BMC Software.

**Note:** There are two versions of IBM Director: IBM Director and IBM Director Multiplatform. They are based on the same code and software components (IBM Director Server, IBM Director Agent, and IBM Director Console), but the two versions are delivered differently. IBM Director comes with IBM xSeries servers and @server BladeCenter products. It also can be purchased for use on non-IBM systems. IBM Director Multiplatform is a system service that can be installed through IBM Virtualization Engine on iSeries, pSeries, and xSeries servers.

---

### IBM Director environment

IBM Director is designed to manage a complex environment that contains numerous servers, desktop computers, workstations, mobile computers (notebook computers), and assorted devices. IBM Director can manage up to 5000 systems.

An IBM Director environment contains the following groups of hardware:

- One or more servers on which IBM Director Server is installed. Such servers are called *management servers*.
- Servers, workstations, desktop computers, and mobile computers that are managed by IBM Director. Such systems are called *managed systems*.
- Network devices, printers, or computers that have Simple Network Management Protocol (SNMP) agents installed or embedded. Such devices are called *SNMP devices*.

Figure 1 shows the hardware in an IBM Director environment.

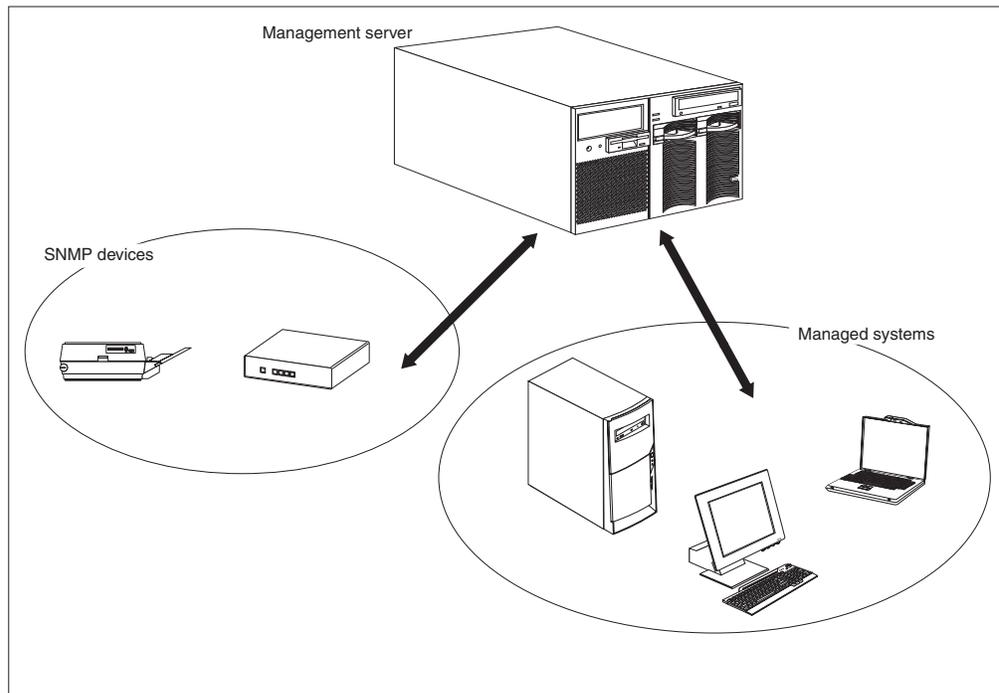


Figure 1. Hardware in an IBM Director environment

---

## IBM Director components

The IBM Director software has three components:

- IBM Director Server
- IBM Director Agent
- IBM Director Console

IBM Director Server must be installed on the management server. When you install IBM Director Server on Microsoft Windows® or Linux, IBM Director Agent and IBM Director Console are installed automatically also. When you install IBM Director Server on IBM i5/OS™, IBM Director Agent is installed automatically also.

IBM Director Agent must be installed on each system that you want to manage.

IBM Director Console must be installed on each system from which a system administrator will remotely access the management server using the graphical user interface (GUI). A system on which IBM Director Console is installed is a *management console*.

Figure 2 shows where the IBM Director software components are installed in a basic IBM Director environment.

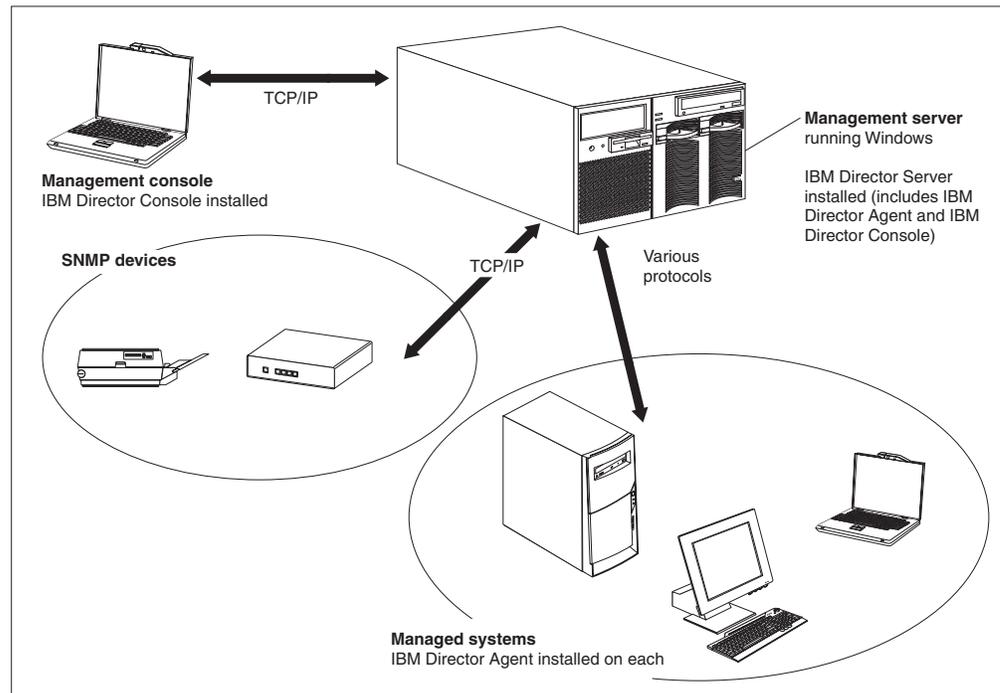


Figure 2. Software in an IBM Director environment

## IBM Director Server

IBM Director Server is the main component of IBM Director; it contains the management data, the server engine, and the application logic. IBM Director Server provides basic functions such as discovery of the managed systems, persistent storage of configuration and management data, an inventory database, event listening, security and authentication, management console support, and administrative tasks.

IBM Director Server stores the inventory data in a Structured Query Language (SQL) database. You can access information that is stored in this relational database even when the managed systems are not available.

Every IBM xSeries server and @server BladeCenter unit comes with an IBM Director Server license. You can purchase additional IBM Director Server licenses for installation on non-IBM servers.

## IBM Director Agent

IBM Director Agent provides management data to IBM Director Server. Data can be transferred using several network protocols, including Transmission Control Protocol/Internet Protocol (TCP/IP), Network Basic Input/Output System (NetBIOS), Internetwork Package Exchange (IPX), and Systems Network Architecture (SNA). IBM Director Server can communicate with all systems in your network that have IBM Director Agent installed.

The IBM Director Agent features vary according to the operating system on which IBM Director Agent is installed. For example, you can install Web-based Access only on Windows 32-bit operating systems.

All IBM @server Intel-compatible servers, IBM @server JS20 blade servers, IBM NetVista™ desktop computers, IBM ThinkCentre™ desktop computers, IBM PC desktop computers, IBM IntelliStation workstations, IBM ThinkPad® mobile computers, IBM TotalStorage® Network Attached Storage (NAS) products, and IBM SurePOS™ point-of-sale systems come with a license for IBM Director Agent. You can purchase additional licenses for non-IBM systems.

## IBM Director Console

IBM Director Console is the GUI for IBM Director Server. Data is transferred between IBM Director Console and IBM Director Server through TCP/IP. Using IBM Director Console, you can conduct comprehensive systems management using either a drop-and-drag action or a single click.

When you install IBM Director Console on a system, IBM Director Agent is not installed automatically. If you want to manage the system on which you have installed IBM Director Console (a management console), you must install IBM Director Agent on that system also.

You may install IBM Director Console on as many systems as needed. IBM Director includes an unlimited-use license for IBM Director Console.

---

## IBM Director Agent features

When you install IBM Director Agent, you have the opportunity to install the following features.

### ServeRAID Manager

ServeRAID™ Manager works with xSeries servers that contain a ServeRAID adapter or an integrated small computer system interface (SCSI) controller with redundant array of independent disks (RAID) capabilities. Using ServeRAID Manager, you can monitor and manage RAID arrays without taking the servers offline.

**Note:** ServeRAID Manager is not supported on VMware console or guest operating systems.

### Management Processor Assistant Agent

Management Processor Assistant (MPA) Agent works with xSeries and @server servers that contain one of the following service processors or adapters:

- Advanced System Management processor (ASM processor)
- Advanced System Management PCI adapter (ASM PCI adapter)
- Integrated system management processor (ISMP)
- Intelligent Platform Management Interface (IPMI) baseboard management controller
- Remote Supervisor Adapter
- Remote Supervisor Adapter II

You must install MPA Agent in order to use the MPA task to configure, monitor, and manage the service processors.

MPA Agent handles in-band communication between service processors and IBM Director Server. MPA Agent also provides in-band alert notification for certain managed systems running Linux and NetWare. For managed systems running

Linux, if System Health Monitoring is not supported on a server, MPA Agent handles in-band alert notification. For managed systems running NetWare, if supported by the service processor, MPA Agent handles in-band alert notification.

## IBM Director Remote Control Agent

You can use IBM Director Remote Control Agent to perform remote desktop functions on managed systems. From IBM Director Console, you can control the mouse and keyboard of a managed system on which IBM Director Remote Control Agent has been installed. This feature is supported only on Windows 32-bit and 64-bit operating systems.

## Web-based Access

When you install Web-based Access on a managed system, you can access IBM Director Agent and view real-time asset and health information about the managed system from either a Web browser or the Microsoft Management Console (MMC). This feature is supported only on Windows 32-bit operating systems.

## Web-based Access help files

These are the help files for the Web-based Access interface. They provide information about the managed-system data that is available when you use Web-based Access, as well as instructions for performing administrative tasks. Web-based Access is supported only on Windows 32-bit operating systems.

## System Health Monitoring

System Health Monitoring provides active monitoring of critical system functions, including system temperatures, voltages, fan speeds, and power state. It produces and relays hardware alerts to the operating-system event log, IBM Director Server, and other management environments. This feature can be installed only on Windows 32-bit operating systems.

### Notes:

1. For managed systems running Windows, you *must* install System Health Monitoring if you want to monitor the system hardware and send in-band alerts.
2. For managed systems running Linux, System Health Monitoring is supported on some xSeries servers. It is not an installable IBM Director Agent feature but is built into IBM Director Agent.

## SNMP Access and Trap Forwarding

This feature enables SNMP as a protocol for accessing managed-system data. This enables SNMP-based managers to poll managed systems and receive their alerts. If System Health Monitoring is enabled also, this feature enables hardware alerts to be forwarded as SNMP traps.

**Note:** For managed systems running Linux, SNMP Access and Trap Forwarding is not an installable IBM Director Agent feature but is built into IBM Director Agent.

---

## IBM Director extensions

*Extensions* are tools that extend the functionality of IBM Director. IBM Director extensions include the IBM Director Server Plus Pack, IBM Director Software Distribution (Premium Edition), IBM Remote Deployment Manager, IBM Scalable Systems Manager, IBM Virtual Machine Manager, and others.

## IBM Director Server Plus Pack

The IBM Director Server Plus Pack contains a portfolio of tools that extend the functionality of IBM Director. These advanced server-management tools are specifically designed for use on xSeries and Netfinity® servers. The Server Plus Pack contains the following extensions:

- Active™ PCI Manager
- Capacity Manager
- Rack Manager
- Software Rejuvenation
- System Availability

To use the Server Plus Pack extensions, you must install them on the management server, the management console, and any managed systems that are xSeries and Netfinity servers. If you do not have IBM xSeries or Netfinity servers in your IBM Director environment, you do not need to install Server Plus Pack extensions.

The Server Plus Pack components that accompany an installation of IBM Director Server and IBM Director Console are on the *IBM Director* CD. The Server Plus Pack components for an IBM Director Agent installation are on the *IBM Director Server Plus Pack* CD.

**Note:** To finish installing Rack Manager on the management server, you also must install the Rack Manager server component, which is located on the *IBM Director Server Plus Pack* CD.

The *IBM Director Server Plus Pack* CD is offered for purchase at an additional fee. For more information, contact your IBM marketing representative.

Unless otherwise noted, the extensions work with all currently offered xSeries servers.

### Active PCI Manager

Active PCI Manager works with the xSeries 235, 255, 345, 360, 365, 440 and 445 servers and the RXE-100 Remote Expansion Enclosure.

Using Active PCI Manager, you can manage peripheral component interconnect (PCI) and peripheral component interconnect-extended (PCI-X) adapters. Active PCI Manager contains two subtasks: Fault Tolerant Management Interface (FTMI) and Slot Manager (previously released as Active PCI Manager). Using FTMI, you can view network adapters that are members of fault-tolerant groups; you also can perform offline, online, failover, and eject operations on the displayed adapters. Using Slot Manager, you can display information about PCI and PCI-X adapters, analyze PCI and PCI-X performance, and determine the best slots in which to install PCI and PCI-X adapters.

### Capacity Manager

Using Capacity Manager, you can monitor critical resources such as processor utilization, hard disk capacity, memory usage, and network traffic. Capacity Manager can identify current or latent bottlenecks for an individual server or a group of servers. It generates performance-analysis reports that recommend ways to prevent diminished performance or downtime; it also forecasts performance trends.

## **Rack Manager**

Using the Rack Manager drag-and-drop interface, you can build a realistic, visual representation of a rack and its components. By clicking an element in the visual representation, you can access detailed information (such as system health and inventory data) for the rack component.

## **Software Rejuvenation**

Using Software Rejuvenation, you can avoid unplanned system outages due to resource exhaustion. As software runs over long periods of time, operating systems steadily consume resources and might fail to relinquish them properly. This phenomenon (known as resource exhaustion or software aging) can eventually lead to ineffective operation or even system failure. Software Rejuvenation monitors operating-system resources, predicts system outages, and generates resource exhaustion events; after being notified, you can take corrective action before a failure occurs.

You also can use Software Rejuvenation to automate the process of restarting operating systems, applications, and services at convenient times and in advance of actual failures. Because Software Rejuvenation is cluster aware, you can use it to restart a node without taking the cluster offline.

## **System Availability**

Using System Availability, you can document and track server availability. System Availability accurately measures server uptime and downtime and provides several graphical representations of this information. It helps you to notice patterns concerning system availability

## **IBM Director Software Distribution (Premium Edition)**

IBM Director Software Distribution (Premium Edition) adds functions to the IBM Director Software Distribution task. You can use the base IBM Director Software Distribution task to import IBM software and build software packages using the Update Assistant wizard. When you purchase and install IBM Director Software Distribution (Premium Edition), you can accomplish the following additional tasks:

- Import both IBM and non-IBM software and build software packages using the wizards that are designed for the following platforms: AIX®, i5/OS, Linux, and Windows
- Back up or export a software package for use on another management server
- Import a software package that was created by another management server

IBM Software Distribution (Premium Edition) is offered for purchase for an additional fee. For more information, contact your IBM marketing representative.

## **IBM Remote Deployment Manager**

IBM Remote Deployment Manager (RDM) is a flexible and powerful tool for configuring, deploying, and retiring systems. Using RDM, you can accomplish the following deployment tasks:

- Update system firmware
- Modify configuration settings
- Install operating systems
- Back up and recover primary partitions
- Securely erase data from disks

RDM supports both customized and scripted deployments. In addition, because it uses industry-standard protocols to wake and discover target systems, RDM does not require an agent component.

RDM is offered for purchase for an additional fee. For more information, contact your IBM marketing representative.

## IBM Scalable Systems Manager

You can use Scalable Systems Manager (SSM) for viewing, configuring, and managing static hardware partitions on supported xSeries servers. Using Scalable Systems Manager, you can perform the following tasks:

- View information about predefined scalable systems and scalable partitions that is saved in non-volatile random access memory (NVRAM)
- Configure and manage additional scalable systems and scalable partitions
- Configure RXE-100 Remote Expansion Enclosures that are attached to servers that are used in scalable partitions

Because SSM communicates with servers out-of-band through their service processor, it does not require an agent component.

You can download SSM from the IBM Support Web site.

## IBM Virtual Machine Manager

IBM Virtual Machine Manager (VMM) enables the use of VMware VirtualCenter and Microsoft Virtual Server in an IBM Director environment. When VMM and these virtualization applications are installed, you can perform the following tasks from IBM Director Console:

- Correlate relationships between physical platforms and virtual components
- Report status of physical platforms and their corresponding virtual components
- Log in to the management interface of the virtualization application
- Discover virtual components
- Perform power operations on virtual machines
- Create event action plans that involve virtual objects

Additionally, for environments running VMware VirtualCenter, VMM provides the ability to move a running virtual machine between two physical hosts.

## Additional IBM Director extensions

IBM provides additional IBM Director extensions that you can download from the IBM Support Web site:

### **Cluster Systems Management**

Enables you to manage IBM Cluster Systems Management (CSM) clusters using IBM Director Console

### **Electronic Service Agent**

Tracks and captures system-inventory data, and if the system is under a service agreement or within the warranty period, automatically reports hardware problems to IBM

### **Real Time Diagnostics**

Enables you to run industry-standard diagnostic utilities on xSeries servers while they are running

IBM can add or withdraw extensions on the IBM Support Web site without notice.

---

## Licensing

Every IBM xSeries server and @server BladeCenter unit comes with an IBM Director Server license. This license includes authorizations for the following installations:

- One installation of IBM Director Server
- 20 installations of IBM Director Agent on non-IBM systems
- Unlimited installations of IBM Director Console

Most IBM Intel-compatible systems come with a license for IBM Director Agent. For a complete list of IBM Intel-compatible systems and @server JS20 blade servers that are entitled to an IBM Director Agent license, see the *IBM Director Hardware and Software Compatibility* document. You can download this PDF file from the IBM Director Agent Web page at [http://www.ibm.com/pc/ww/eserver/xseries/systems\\_management/nfdir/agent.html](http://www.ibm.com/pc/ww/eserver/xseries/systems_management/nfdir/agent.html).

You can purchase additional licenses for non-IBM systems, if needed. For more information, contact your IBM marketing representative.

The license to install IBM Director Server also includes the right to install the Server Plus Pack on the management server. This allows you to use the Server Plus Pack extensions (except for Rack Manager) on the management server *only*. To install the Server Plus Pack on managed systems or Rack Manager on the management server, you must purchase additional licenses. Contact your IBM marketing representative for more information.

---

## Upgrading from previous releases of IBM Director

If you are running one of the following versions of IBM Director on a supported operating system, you can upgrade to IBM Director 4.20:

- IBM Director 3.1
- IBM Director 3.1.1
- IBM Director 4.1
- IBM Director 4.10.2
- IBM Director 4.11
- IBM Director 4.12

Versions of IBM Director earlier than IBM Director 3.1 are not compatible with IBM Director 4.20.

IBM Director Server 4.20 can manage systems running IBM Director Agent, version 3.1 or later. This enables you to manage systems that are running operating systems that are not supported by IBM Director 4.20.

IBM Director Server and IBM Director Console must be at the same release level. If you upgrade IBM Director Server, you must upgrade IBM Director Console also.

If IBM Director Console and IBM Director Agent are installed on the same system, both software components must be at the same release level as IBM Director Server.

If the IBM SMBus device driver for Linux, version 4.1, 4.11, or 4.12, is installed on a managed system, you must uninstall the device driver and then install the IBM SMBus device driver, version 4.20.



---

## Chapter 2. Requirements for installing IBM Director

This chapter contains information about hardware requirements, supported operating systems, network protocols, and supported database applications. It also contains an overview of the IBM Director security features.

---

### Hardware requirements

This section contains information about the minimum requirements that must be met when you install IBM Director.

Because a system configured with the minimum requirements might perform poorly in a production environment, consider the following suggestions:

- The microprocessor speed, memory, and disk space minimum requirements are *in addition* to whatever resources are necessary for the software already installed on the system.
- Conduct a performance analysis to ensure that the system has sufficient capacity to handle the additional requirements of functioning as a management server or a management console

### Intel-compatible systems and eServer JS20 blade servers

The systems on which you install IBM Director Agent or IBM Director Server must meet the Wired for Management (WfM), version 2.0, specifications.

The following table lists the minimum microprocessor speed, random access memory (RAM), and disk space needed by the IBM Director components.

*Table 1. Intel-compatible systems and eServer JS20 blade servers: Minimum hardware requirements*

Requirements	IBM Director Agent	IBM Director Console	IBM Director Server
Microprocessor speed	Pentium®-class or Itanium 2 processor	Pentium 300 megahertz (MHz)	Pentium 300 MHz
Memory (RAM)	128 megabyte (MB)	128 MB	256 MB (512 MB recommended)
Disk space	43-109 MB	168 MB	316 MB
Display	Not applicable	At least 256 colors	At least 256 colors

The amount of disk space that is required for an IBM Director Agent installation depends on the operating system:

- AIX 5L, Version 5.2 requires 43 MB.
- Red Hat® Enterprise Linux AS, version 3.0, for IBM PowerPC® (iSeries and pSeries) and SUSE LINUX Enterprise Server 8 for IBM pSeries and IBM iSeries require 88 MB.
- All other supported operating systems require 109 MB.

In addition, System Management BIOS (SMBIOS) 2.1 or later is required for all systems in an IBM Director environment.

## iSeries servers

The following table lists the minimum commercial processing workload (CPW), storage pool size, and disk space needed by the IBM Director components.

Table 2. iSeries servers: Minimum hardware requirements

Requirements	IBM Director Agent	IBM Director Server
Relative system performance	75 CPW	150 CPW
Storage pool size	350 MB	500 MB
Disk space	300 MB	500 MB

The following table lists the products or options that are required to successfully install and securely run IBM Director.

Table 3. iSeries servers: Required products and options

Products or options	Order number
IBM Cryptographic Access Provider 128-bit for iSeries	5722-AC3
IBM HTTP Server for iSeries	5722-DG1
Option 5, Java™ Developer Kit 1.3	5722-JV1
Option 30, OS/400® - Qshell	5722-SS1
Option 34, OS/400 - Digital Certificate Manager	5722-SS1

---

## Supported operating systems

This section lists the operating systems upon which IBM Director Server, IBM Director Agent, IBM Director Console, and the Server Plus extensions are supported.

Consider the following restrictions concerning operating-system support:

- To install IBM Director Agent on the following operating systems, you can use either IBM Director Multiplatform or the IBM Director software that came with your BladeCenter unit:
  - AIX 5L, Version 5.2
  - Red Hat Enterprise Linux AS, version 3.0, for IBM PowerPC (iSeries and pSeries)
  - SUSE LINUX Enterprise Server 8 for IBM pSeries and IBM iSeries

The software for these installations also can be downloaded from the IBM Support Web site.

- To install IBM Director Agent or IBM Director Server on i5/OS (formerly OS/400), you must use IBM Director Multiplatform, which is installed using the IBM Virtualization Engine.

For the most recent list of supported operating systems, see the *IBM Director Hardware and Software Compatibility* document. This PDF file is updated every 6 to 8 weeks. You can download it from [http://www.ibm.com/servers/eserver/xseries/systems\\_management/sys\\_migration/ibmdiragent.html](http://www.ibm.com/servers/eserver/xseries/systems_management/sys_migration/ibmdiragent.html).

## IBM Director Server

You can install IBM Director Server on the following operating systems:

- i5/OS, Version 5 Release 3
- Red Hat Linux Advanced Server, version 2.1 (Update 3 required)
- Red Hat Enterprise Linux AS, version 2.1 (Update 3 required)
- Red Hat Enterprise Linux AS, version 3.0, for Intel x86
- Red Hat Enterprise Linux ES, versions 2.1 and 3.0
- SUSE LINUX Enterprise Server 8 for x86 (Service Pack 3 required)
- Windows 2000, Advanced Server and Server Editions (Service Pack 3 required)
- Windows Server 2003, Enterprise, Standard, and Web Editions

## IBM Director Agent

You can install IBM Director Agent on the following operating systems:

- AIX 5L, Version 5.2 (Recommended Maintenance Package 5.2.00-03 or later required)
- i5/OS, Version 5 Release 3
- Novell NetWare, versions 6.0 and 6.5
- Red Hat Linux Advanced Server, version 2.1 (Update 3 required)
- Red Hat Enterprise Linux AS, version 2.1 (Update 3 required)
- Red Hat Enterprise Linux AS, version 3.0, for Intel x86
- Red Hat Enterprise Linux ES and WS, versions 2.1 and 3.0
- Red Hat Enterprise Linux AS, version 3.0, for AMD64 (64-bit)
- Red Hat Enterprise Linux AS, version 3.0, for IBM PowerPC (iSeries and pSeries)
- Red Hat Enterprise Linux AS, version 3.0, for Intel Itanium (64-bit)
- SUSE LINUX Enterprise Server 8 for AMD64 (Service Pack 3 required)
- SUSE LINUX Enterprise Server 8 for IBM pSeries and IBM iSeries (Service Pack 3 required)
- SUSE LINUX Enterprise Server 8 for Itanium Processor Family (Service Pack 3 required)
- SUSE LINUX Enterprise Server 8 for x86 (Service Pack 3 required)
- VMware ESX Server, version 1.5.2 (Patch 3 required) with the following guest operating systems:
  - Red Hat Linux Advanced Server, version 2.1 (Update 3 required)
  - Windows NT<sup>®</sup> 4.0 Workstation (Service Pack 6a or later required)
  - Windows NT 4.0 Server, Enterprise and Standard Editions (Service Pack 6a or later required)
  - Windows 2000, Advanced Server, Professional, and Server Editions (Service Pack 3 or later required)
  - Windows Server 2003, Enterprise, Standard, and Web Editions
- VMware ESX Server, version 2.0, with the following guest operating systems:
  - Red Hat Linux Advanced Server, version 2.1 (Update 3 required)
  - Red Hat Enterprise Linux AS, version 2.1 (Update 3 required)
  - SUSE LINUX Enterprise Server 8 for x86 (Service Pack 3 required)
  - Windows NT 4.0 Server (Service Pack 6a or later required)

- Windows 2000, Advanced Server, Professional, and Server Editions (Service Pack 3 or later required)
- Windows Server 2003, Enterprise, Standard, and Web Editions
- VMware ESX Server, version 2.0.1, with the following guest operating systems:
  - Red Hat Linux Advanced Server, version 2.1 (Update 3 required)
  - Red Hat Enterprise Linux AS, versions 2.1 (Update 3 required)
  - Red Hat Enterprise Linux AS, version 3.0, for Intel x86
  - SUSE LINUX Enterprise Server 8 for x86 (Service Pack 3 required)
  - Windows NT 4.0 Server (Service Pack 6a or later required)
  - Windows 2000, Advanced Server, Professional, and Server Editions (Service Pack 3 or later required)
  - Windows Server 2003, Enterprise, Standard, and Web Editions
- VMware ESX Server, version 2.1, with the following guest operating systems:
  - Red Hat Enterprise Linux AS, version 2.1 (Update 3 required)
  - Red Hat Enterprise Linux AS, version 3.0, for Intel x86
  - SUSE LINUX Enterprise Server 8 for x86 (Service Pack 3 required)
  - Windows NT 4.0 Server (Service Pack 6a or later required)
  - Windows 2000, Advanced Server and Server Editions (Service Pack 3 or later required)
  - Windows XP Professional Edition (Service Pack 1 required)
  - Windows Server 2003, Enterprise, Standard, and Web Editions
- Windows NT 4.0 Workstation (Service Pack 6a or later required)
- Windows NT 4.0 Server, Standard, Enterprise, and Terminal Server Editions (Service Pack 6a or later required)
- Windows NT 4.0 Server with Citrix MetaFrame (Service Pack 6a or later required)
- Windows 2000, Advanced Server, Datacenter Server, Professional, and Server Editions (Service Pack 3 or later required)
- Windows XP Professional Edition (Service Pack 1 or 1a recommended)
- Windows Server 2003, Enterprise, Datacenter, Standard, and Web Editions
- Windows Server 2003, Datacenter and Enterprise Editions, 64-bit versions

## IBM Director Console

You can install IBM Director Console on the following operating systems:

- Red Hat Linux Advanced Server, version 2.1 (Update 3 required)
- Red Hat Enterprise Linux AS, version 2.1 (Update 3 required)
- Red Hat Enterprise Linux AS, version 3.0, for Intel x86
- Red Hat Enterprise Linux ES, versions 2.1 and 3.0
- SUSE LINUX Enterprise Server 8 for x86 (Service Pack 3 required)
- Windows 2000, Advanced Server, Professional, and Server Editions (Service Pack 3 required)
- Windows XP Professional Edition (Service Pack 1 or 1a recommended)
- Windows Server 2003, Enterprise, Standard, and Web Editions

## Server Plus Pack extensions

The following table lists the Server Plus Pack extensions and the operating systems on which they are supported.

Table 4. Supported operating systems for Server Plus Pack extensions installed on managed systems

Operating system	Version and release	Active PCI Manager	Capacity Manager	Rack Manager	Software Rejuvenation	System Availability
<b>Linux</b>						
Red Hat Enterprise Linux, 2.1 and 3.0 for x86	AS ES	No	Yes	Yes	Yes	Yes
	WS	No	No	Yes	No	No
Red Hat Enterprise Linux AS, 3.0	AMD64 IBM PowerPC (iSeries and pSeries) Intel Itanium	No	No	No	No	No
SUSE LINUX Enterprise Server 8	For x86	Yes <sup>1</sup>	Yes	Yes	Yes	Yes
	AMD64	No	No	No	No	No
	IBM pSeries and iSeries	No	No	Yes	No	No
	Itanium Processor Family	No	No	No	No	No
VMware ESX Server	Versions 1.5.2, 2.0, 2.0.1, and 2.1 Console	No	Yes	No	No	Yes
	Versions 1.5.2, 2.0, 2.0.1, and 2.1 Guest operating systems	No	Yes	No	Yes	Yes
<b>Other</b>						
AIX 5L	Version 5.2	No	No	No	No	No
i5/OS	Version 5 Release 3	No	No	No	No	No
NetWare	Versions 6.0 and 6.5	No	Yes	Yes	No	No
<b>Windows</b>						
Windows NT 4.0	Workstation	No	No	Yes	No	No
	Server, Standard Edition Server, Enterprise Edition	No	Yes	Yes	Yes	Yes
	Server, Terminal Server Edition Server, with Citrix MetaFrame	No	No	Yes	No	No
Windows 2000	Professional Edition	No	No	Yes	No	No
	Server Edition Advanced Server Edition Datacenter Server Edition	Yes	Yes	Yes	Yes	Yes
Windows XP	Professional Edition	No	No	Yes	No	No
Windows Server 2003	Standard Edition Enterprise Edition Web Edition	Yes <sup>1</sup>	Yes	Yes	Yes	Yes
	Datacenter Edition	Yes <sup>1</sup>	Yes	Yes	Yes	Yes
	For 64-bit Itanium systems: Enterprise Edition Datacenter Edition	No	No	No	No	No
<sup>1</sup> Slot Manager only						

---

## Network requirements

This section discusses supported network protocols and the ports used in an IBM Director environment.

## Network protocols

The following table lists the versions of network protocols that can be used in an IBM Director environment.

*Table 5. Supported versions of network protocols*

Protocol	Supported version
IPX	IPX versions supported by NetWare and Windows
NetBIOS	Native NetBIOS versions supported by Windows
SNA	Microsoft SNA 4.0 with Service Pack 1
TCP/IP	All WinSock-compatible versions of TCP/IP version 4.0 supported by AIX, i5/OS, Linux, NetWare, and Windows

Some network protocols are supported only for certain types of data transmissions or on certain operating systems. The following table contains additional information.

*Table 6. Types of data transmission and supported network protocols*

Type of data transmission	Operating system running on managed system	Supported network protocols
IBM Director Server ↔ IBM Director Console	Not applicable	TCP/IP
IBM Director Server ↔ SNMP devices	Not applicable	TCP/IP
IBM Director Server ↔ IBM Director Agent	AIX	TCP/IP
	i5/OS	TCP/IP
	Linux	TCP/IP
	NetWare	IPX or TCP/IP
	Windows	IPX, NetBIOS, SNA, or TCP/IP

## Ports

The following table lists the ports used in an IBM Director environment. The abbreviations that appear in this table are spelled out at the bottom of the table.

Table 7. Ports used by IBM Director

Category	Connection	Destination port
<b>IBM Director interprocess communication</b>	IBM Director Server ↔ IBM Director Agent	14247 UDP and TCP 14248 UDP (i5/OS and Linux) 4490 IPX (read) 4491 IPX (write)
	IBM Director Console → IBM Director Server	2033 TCP <sup>1</sup>
	DIRCMD client ↔ IBM Director Server	2034 TCP
	IBM Director Console → IBM Director Console	a free port (For use of BladeCenter Switch Management launch pad)
	Web-based Access (Configured during installation of IBM Director Agent)	411 HTTP (default) 423 HTTPS (default)  8009 (internal use)
<b>HTTP</b>	IBM Director Server → BladeCenter switch module	80 TCP
	Web-based Access	80 HTTP
<b>Service processors</b>	IBM Director Server ↔ service processor	6090 TCP
	Service processor → IBM Director Server (alerts)	13991 UDP
	IBM Director Server → service processor (ASF, ASF 2.0, and IPMI)	623 and 664 UDP
	Service processor → IBM Director Server (ASF, ASF 2.0, and IPMI)	Random port in the 1024-65535 range <sup>2</sup>
<b>SNMP</b>	IBM Director Server → SNMP agent	161 UDP
	SNMP agent → IBM Director Server	162 UDP
<b>SSH</b>	IBM Director Server → SNMP devices (Remote Session task)	22 TCP
<b>Telnet</b>	IBM Director Server → BladeCenter management module	23 TCP
	IBM Director Server → BladeCenter switch module	23 TCP
	IBM Director Server → SNMP devices (Remote Session task)	23 TCP

<sup>1</sup> IBM Director Console opens a random port in the 1024-65535 range and then connects to IBM Director Server on port 2033. When IBM Director Server responds to IBM Director Console, it connects to the random port in the 1024-65535 range.

<sup>2</sup> You can specify a fixed port by modifying the `asmDefinitions.properties` file, which is in the data directory.

**Abbreviations:** ASF = Alert Standard Format; HTTP = Hypertext Transfer Protocol; HTTPS = Hypertext Transfer Protocol Secure; IPMI= Intelligent Platform Management Interface; SNMP = Simple Network Management Protocol; SSH = Secure Shell; TCP = Transmission Control Protocol; UDP = User Datagram Protocol

---

## Supported Web browsers for Web-based Access

If you have installed Web-based Access on a managed system, you can use the following Web browsers to access a managed system:

- Microsoft Internet Explorer, version 4.01 or later
- Netscape Navigator, version 4.7x
- Netscape Navigator, version 7.01 or later

You also can use Microsoft Management Console (MMC), version 1.1 or later.

### Notes:

1. Your Web browser must support Java applets.
2. If you are using Internet Explorer, you must use 56-bit encryption or higher.

---

## Supported database applications

IBM Director Server requires a SQL database to store the system inventory data. The following table lists the database applications supported for use with IBM Director Server.

*Table 8. Database applications supported by IBM Director*

Operating system running on the management server	Database application
i5/OS	IBM DB2 <sup>®</sup> Universal Database <sup>™</sup> for iSeries
Linux	IBM DB2 Universal Database 8.1, Fix Pack 5
	Oracle Server, versions 8.1.7, 9.0, and 9.2
	PostgreSQL, versions 7.2.x and 7.3.x
Windows	IBM DB2 Universal Database 8.1, Fix Pack 5
	Microsoft Jet 4.0 database engine, with Service Pack 8
	Microsoft Data Engine (MSDE) 2000, with Service Pack 3a
	Microsoft SQL Server 2000 Desktop Engine, with Service Pack 3a
	Microsoft SQL Server 2000, with Service Pack 3a
	Oracle Server, versions 8.1.7, 9.0, and 9.2

**Note:** If both the following conditions are true, make sure the Microsoft Data Access Control (MDAC) 2.8 is installed on the same server as the database application:

- The database server is running Windows 2000.
- You are using one of the Microsoft database applications.

---

## Chapter 3. Planning your IBM Director installation

This chapter contains information about planning your IBM Director environment. It also includes information about working with service processors, setting up a BladeCenter deployment infrastructure, and preparing a database for use with IBM Director.

---

### General planning considerations

This sections contains information about the following topics:

- Reviewing your environment
- Selecting on what server to install IBM Director Server
- Selecting the IBM Director database application
- Updating device drivers, firmware, and basic input/output system (BIOS) code

### Reviewing your environment

Review the environment that you want to manage with IBM Director. Your network must be up and running before you install IBM Director. Complete the following tasks to facilitate the IBM Director installation and discovery of systems and devices:

- Determine the physical locations and network addresses of all systems and devices in your network. Identify local and remote subnets and the network protocols that are used.
- Determine the amount of traffic that your network can manage. If you have a wide area network (WAN) link, use *at least* a 1.5 megabytes per second (MBps) T1 line to ensure reliable network performance.
- Ensure that all systems and devices are properly installed and cabled.
- Enable SNMP traps, if necessary. If you want IBM Director to poll SNMP devices and receive their alerts, make sure that an SNMP server and an SNMP trap service are running on the management server.

### Selecting where to install IBM Director Server

Determine the server on which you will install IBM Director Server.

You must use a non-blade server as the management server. This ensures that you can run the BladeCenter Deployment wizard and use the BladeCenter tasks.

(Windows installations) Do not install IBM Director Server on a domain controller. Its high resource utilization might degrade domain controller performance. In addition, if you install IBM Director Server on a domain controller and then demote the domain controller, you no longer can access IBM Director Console. Furthermore, unless the IBM Director service account has domain administrator privileges, you cannot restart IBM Director Server.

Depending on the following considerations, you might want to install more than one instance of IBM Director Server:

- You want to manage more than 5000 systems.
- The systems that you want to manage are in several geographic locations or are owned by multiple system administrators.

## Selecting the IBM Director database application

If you plan to install IBM Director Server on i5/OS, you do not need to select a database application. IBM DB2 Universal Database for iSeries is built into i5/OS. However, if you plan to install IBM Director Server on Linux or Windows, you must select the database application that you will use with IBM Director.

See “Preparing the IBM Director database” on page 28 for more information.

## Updating device drivers, firmware, and BIOS code

Consider updating the device drivers, firmware, and BIOS code on the systems that you plan to manage before you install IBM Director Agent. Updating the device drivers, firmware, and BIOS code will ensure that the latest performance improvements and fixes are applied.

You can use *UpdateXpress* to perform such updates on xSeries servers and certain Netfinity servers. Be sure to check the supported servers information located on the *UpdateXpress* CD before you use the CD to install updates.

---

## Managing service processors

To effectively use IBM Director to manage IBM Netfinity and xSeries servers, you must identify which service processors are present in the servers. This enables you to accomplish the following tasks:

- Determine which IBM Director Agent features and Linux device drivers to install on managed systems
- Decide how to configure servers, optional service processors, and Advanced System Management (ASM) interconnects to maximize the ability of systems to communicate with and send alerts to IBM Director Server
- Manually create management processor objects in IBM Director Console, if needed

## Communication between service processors and IBM Director Server

There are several pathways along which communication between IBM Director Server and the service processors present in IBM Netfinity or xSeries servers takes place:

### In-band communication

IBM Director Server communicates with IBM Director Agent; IBM Director Agent uses a device driver to pass data to and from the service processor. This also is called interprocess communication (IPC).

### Over the local area network (LAN)

Data is transmitted between the service processor and IBM Director Server over the LAN. This is possible if the service processor has an integrated network interface card (NIC) or access to a NIC shared with the server.

### Over the ASM interconnect

Data is passed from the service processor over an ASM interconnect network to a second service processor. The second service processor serves as a gateway between IBM Director Server and the first service processor.

Both of the latter types of communication are known as *out-of-band* communication, because they take place independent of an operating system.

An *ASM interconnect network* is a group of service processors networked together using the ASM interconnect feature. Connected through the RS-485 ports, the service processors can communicate with and send alerts out-of-band to IBM Director Server through a *gateway service processor* (sometimes called an ASM interconnect gateway). An ASM interconnect network eliminates the need for multiple modems, telephones, and LAN ports; it also permits service processors without network interface cards to communicate out-of-band with IBM Director Server.

**Notes:**

1. For IBM Director and Scalable Systems Manager (SSM) to communicate out-of-band, the following conditions must be met:
  - Service processors must maintain consistent IP addresses. You either must assign static IP addresses or configure Dynamic Host Configuration Protocol (DHCP) to maintain consistent IP addresses for the service processors.
  - The service processor IP addresses cannot change after IBM Director has discovered the server.
2. Only one of the following systems management applications can communicate with a service processor at any given time:
  - Cluster Systems Management (CSM)
  - IBM Director Server
  - IBM Management Processor Command-Line Interface (MPCLI)

## In-band communication and alerts

To enable in-band communication between IBM Director Server and a managed system that contains a service processor, both the service processor device driver and MPA Agent must be installed on the managed system.

Whether a service processor can communicate in-band with IBM Director Server depends on both the type of service processor and the operating system running on the managed system.

*Table 9. In-band communication between service processors and IBM Director Server*

Primary service processor	Operating system		
	Linux	NetWare	Windows
Advanced System Management PCI Adapter (ASM PCI Adapter)	Yes	Yes	Yes
Advanced System Management processor (ASM processor)	Yes	Yes	Yes
Integrated system management processor (ISMP)	Yes	No	Yes
IPMI baseboard management processor	Yes	No	Yes
Remote Supervisor Adapter	Yes	Yes	Yes
Remote Supervisor Adapter II	Yes	Yes <sup>1</sup>	Yes
<sup>1</sup> Novell NetWare 6.5 only			

When in-band communication is possible, alerts are handled either by MPA Agent or System Health Monitoring. Unless the server supports System Health Monitoring, ISMPs in servers running Linux cannot send alerts in-band, although in-band communication between the service processor and IBM Director Server is possible.

The following table specifies which IBM Director Agent feature handles in-band alerting.

Table 10. IBM Director Agent features that handle in-band alerts

Type of service processor	Operating system running on managed system		
	Linux	NetWare	Windows
ASM PCI Adapter	MPA Agent	MPA Agent	System Health Monitoring
ASM processor	MPA Agent	MPA Agent	System Health Monitoring
ISMP	None or System Health Monitoring <sup>1</sup>	Not applicable	System Health Monitoring
IPMI baseboard management processor	System Health Monitoring	Not applicable	System Health Monitoring
Remote Supervisor Adapter	MPA Agent or System Health Monitoring <sup>2</sup>	MPA Agent	System Health Monitoring
Remote Supervisor Adapter II	MPA Agent or System Health Monitoring <sup>2</sup>	MPA Agent	System Health Monitoring
<sup>1</sup> If System Health Monitoring is supported on the server. <sup>2</sup> MPA Agent handles the alerts, unless System Health Monitoring is supported on the server.			

See the *IBM Director Hardware and Software Compatibility* document for a list of servers on which System Health Monitoring is supported when the server is running Linux. This PDF file is updated every 6 to 8 weeks. You can download it from [http://www.ibm.com/servers/eserver/xseries/systems\\_management/sys\\_migration/ibmdiragent.html](http://www.ibm.com/servers/eserver/xseries/systems_management/sys_migration/ibmdiragent.html).

## Out-of-band communication and alerts

The type of service processor present in a server determines which paths out-of-band communication can take. Servers that contains ISMPs can only communicate out-of-band with IBM Director Server through a gateway service processor.

### Gateway service processors

The following service processors all can serve as gateway service processors:

- ASM PCI Adapter
- ASM processor
- Remote Supervisor Adapter
- Remote Supervisor Adapter II

However, some of these service processors cannot communicate with certain other service processors. In addition, an ASM processor can communicate with IBM Director Server only through interprocess communication

The following table details the possible gateway service processors and the types of service processors located on an ASM interconnect network with which they can communicate.

*Table 11. Gateway service processors and communication with service processors on an ASM interconnect network*

Gateway service processor	Service processor on an ASM interconnect					
	ASM processor	ASM PCI adapter	ISMP	IPMI baseboard management controller	Remote Supervisor Adapter	Remote Supervisor Adapter II
ASM PCI adapter	Yes	Yes	No	Not applicable	No	No
ASM processor	Yes	Yes	No	Not applicable	No	No
Remote Supervisor Adapter	Yes	Yes	Yes	Not applicable	Yes	Yes
Remote Supervisor Adapter II	Yes	Yes	Yes	Not applicable	Yes	Yes

To maximize the possibility of IBM Director Server receiving alerts from service processors located on an ASM interconnect network, consider using a Remote Supervisor Adapter or a Remote Supervisor Adapter II as a gateway service processor.

**Note:** If you have one of the following servers attached to an RXE-100 Remote Expansion Enclosure, you cannot use the on-board Remote Supervisor Adapter as a gateway service processor:

- xSeries 360
- xSeries 365
- xSeries 440
- xSeries 445
- xSeries 455

The Remote Supervisor Adapter is dedicated to managing the RXE-100 Remote Expansion Enclosure.

## Alerting and alert-forwarding strategies

The following table contains information about the pathways available for out-of-band alerting.

Table 12. Out-of-band alerting pathways

Type of service processor	Pathways for out-of-band alerting	Possible gateway service processors
ASM PCI adapter	<ul style="list-style-type: none"> <li>LAN</li> <li>Over an ASM interconnect</li> </ul>	<ul style="list-style-type: none"> <li>ASM PCI adapter</li> <li>Remote Supervisor Adapter</li> <li>Remote Supervisor Adapter II</li> </ul>
ASM processor	<ul style="list-style-type: none"> <li>Over an ASM interconnect</li> </ul>	<ul style="list-style-type: none"> <li>ASM PCI adapter</li> <li>Remote Supervisor Adapter</li> <li>Remote Supervisor Adapter II</li> </ul>
ISMP	<ul style="list-style-type: none"> <li>Over an ASM interconnect</li> </ul>	<ul style="list-style-type: none"> <li>Remote Supervisor Adapter</li> <li>Remote Supervisor Adapter II</li> </ul>
IPMI baseboard management processor	<ul style="list-style-type: none"> <li>LAN</li> </ul>	<ul style="list-style-type: none"> <li>Not applicable</li> </ul>
Remote Supervisor Adapter	<ul style="list-style-type: none"> <li>LAN</li> <li>Over an ASM interconnect</li> </ul>	<ul style="list-style-type: none"> <li>Remote Supervisor Adapter</li> <li>Remote Supervisor Adapter II</li> </ul>
Remote Supervisor Adapter II	<ul style="list-style-type: none"> <li>LAN</li> <li>Over an ASM interconnect</li> </ul>	<ul style="list-style-type: none"> <li>Remote Supervisor Adapter</li> <li>Remote Supervisor Adapter II</li> </ul>

See the documentation that came with the server for information about how to configure your service processor and ASM interconnect to ensure that IBM Director Server receives alerts. The IBM Redbooks publication *Implementing Systems Management Solutions Using IBM Director* (SG24-6188-01) also contains information that might be helpful. See “IBM Director documentation” on page xiv for more information.

The type of service processor also determines what type of alert-forwarding strategy is possible. The following table contains information about possible alert-forwarding strategies.

Table 13. Out-of-band alert-forwarding strategies

Type of service processor	Possible alert-forwarding strategies
ASM PCI adapter	IBM Director over LAN
ASM processor	IBM Director over LAN
ISMP	Not applicable
IPMI baseboard management processor	IBM Director comprehensive
Remote Supervisor Adapter	IBM Director over LAN IBM Director comprehensive
Remote Supervisor Adapter II	IBM Director comprehensive

Some service processors also support SNMP as an alert-forwarding strategy.

## Setting up a BladeCenter deployment infrastructure

**Important:** If you want to use IBM Director to manage the blade servers in a BladeCenter chassis, you must use a non-blade server as the management server.

Consider setting up a separate management network to configure and manage your BladeCenter chassis and blade servers. By separating the LAN segment used for production from the LAN segment to which the BladeCenter management module is connected, you can ensure that only authorized system administrators can connect to the BladeCenter chassis and switch modules.

Figure 3 shows a network that you could use to securely deploy your BladeCenter chassis and blade servers.

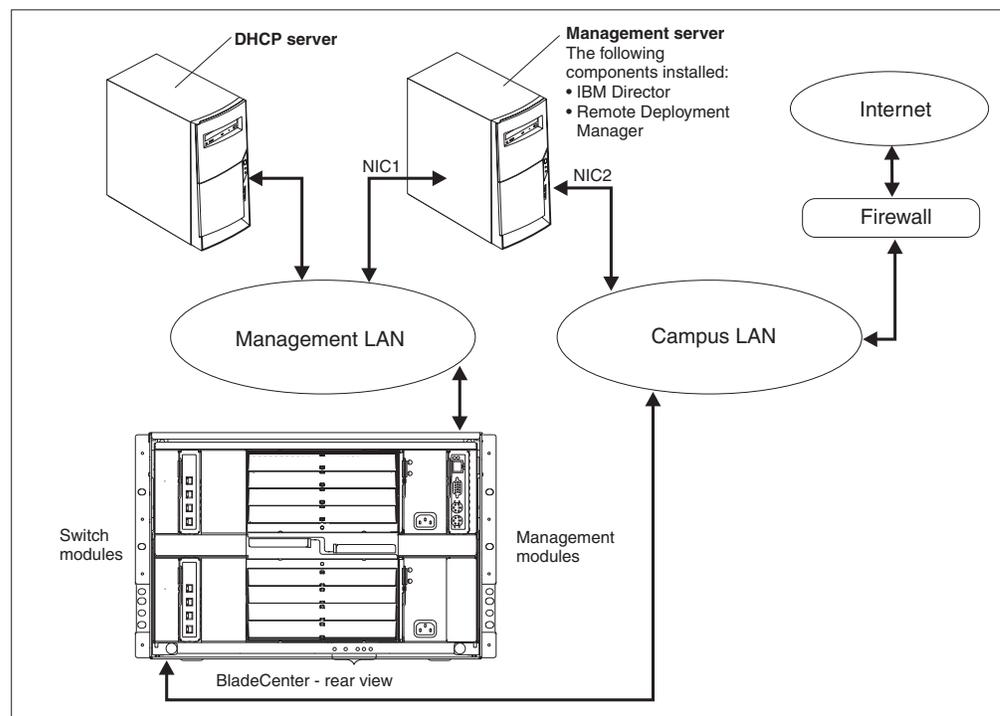


Figure 3. Example of a BladeCenter deployment network

Such a network configuration ensures that applications running on the blade servers cannot modify chassis settings, because the blade servers have no connection to either the management module or the switch module configuration ports.

Consider using a Dynamic Host Configuration Protocol (DHCP) server to assign an address to the external port of the management module. When a BladeCenter management module is first started, it searches for a DHCP server. If a DHCP server is not found, the BladeCenter management module assigns IP address 192.168.70.125 to the external management port. Because this static IP address is the same for all management modules, IP address conflicts can occur if you do not use a DHCP server and introduce multiple BladeCenter chassis onto a network simultaneously. When you configure the BladeCenter chassis, you assign static IP addresses to the switch module and the external and internal ports of the management module.

If you intend to use Remote Deployment Manager (RDM), install RDM on the management server also.

(Windows only) If you plan to use a database application other than Microsoft Jet, consider installing the database server on the management LAN also. If the database server is in a different domain, there must be a trust relationship between the two domains.

Make sure that you have installed the latest version of the management module firmware. To download the firmware, go to the IBM Support Web site at <http://www.ibm.com/pc/support/>.

Only one of the following software applications can communicate with a BladeCenter management module at any given time:

- Cluster Systems Management (CSM)
- IBM Director Server
- IBM Management Processor Command-Line Interface (MPCLI)

---

## Preparing the IBM Director database

IBM Director Server uses a SQL database to store the system inventory data. The following table lists the database applications supported for use with IBM Director Server.

Operating system running on the management server	Database application
i5/OS	IBM DB2 Universal Database for iSeries
Linux	IBM DB2 Universal Database 8.1, Fix Pack 5
	Oracle Server, versions 8.1.7, 9.0, and 9.2
	PostgreSQL, versions 7.2.x and 7.3.x
Windows	IBM DB2 Universal Database 8.1, Fix Pack 5
	Microsoft Jet 4.0 database engine, with Service Pack 8
	Microsoft Data Engine (MSDE) 2000, with Service Pack 3a
	Microsoft SQL Server 2000 Desktop Engine, with Service Pack 3a
	Microsoft SQL Server 2000, with Service Pack 3a
	Oracle Server, versions 8.1.7, 9.0, and 9.2

**Note:** If both the following conditions are true, make sure the Microsoft Data Access Control (MDAC) 2.8 is installed on the same server as the database application:

- The database server is running Windows 2000.
- You are using one of the Microsoft database applications.

Unless you plan to use IBM DB2 Universal Database for iSeries or Microsoft Jet, the database application must be installed before you install IBM Director Server.

Consider the following information:

- The database administrator should determine an appropriate size for the database file. If the IBM Director environment will be 300 to 500 systems, an initial size of 100 MB is sufficient. A larger database might be necessary if there will be additional managed systems or extensive inventory data.
- For IBM DB2, Microsoft SQL Server, and PostgreSQL, the user ID for the IBM Director database must have the following runtime permissions:
  - CREATE TABLE
  - ALTER TABLE
  - DROP TABLE
  - CREATE INDEX
  - ALTER INDEX
  - DROP INDEX
  - CREATE VIEW
  - ALTER VIEW
  - DROP VIEW

## IBM DB2 Universal Database

You can use IBM DB2 Universal Database with management servers running i5/OS, Linux, or Windows. If the management server is running i5/OS, DB2 is already configured for use with IBM Director.

### Management server running Linux

**Note:** If IBM Director will have a remote connection to DB2, you must create a node entry for the database server.

Complete the following steps before installing IBM Director Server:

1. Install DB2 Universal Database, if you have not done so already.
2. Install the DB2 Administration Client Version 8.1 on the management server.
3. Create a DB2 server ID for use with IBM Director.
4. Complete one of the following tasks:
  - Assign the DB2 server ID that you created in step 3 Create Database permission. This allows the DB2 database to be created *during* the installation of IBM Director Server.
  - Create the DB2 database. Either transfer ownership of the database to the DB2 server ID that you created in step 3 or give the DB2 server ID that you created in step 3 the necessary runtime permissions.
5. Provide the following information to the system administrator who will install IBM Director Server:
  - Database name (if a database was created in step 4)
  - Node name (if IBM Director will have a remote connection to DB2)
  - User ID and password, if necessary

## Management server running Windows

### Notes:

1. If IBM Director will have a remote connection to DB2, you must create a node entry for the database server.
2. If the management server and the database server are located in different domains, the following conditions apply:
  - The IBM Director service account must be a domain account.
  - There must be a trust relationship between the domains.

Complete the following tasks before installing IBM Director Server:

1. Install DB2 Universal Database, if you have not done so already.
2. Install the DB2 Administration Client Version 8.1 on the management server. Be sure to install the following components:
  - Base Client Support
  - System Bind Files
  - Java Runtime Environment (JRE)
  - Communication Protocols
3. If you use trusted connections, set the database server security to support trusted connections. See the *DB2 Administration Guide* for information about trusted DB2 client scenarios.
4. Authorize the IBM Director service account to log on to DB2. See the *DB2 Administration Guide* for additional information about DB2 security.
5. Complete one of the following tasks:
  - Assign the IBM Director service account Create Database permission. This allows the DB2 database to be created *during* the installation of IBM Director Server.
  - Create the DB2 database. Either transfer ownership of the database to the IBM Director service account or give the IBM Director service account user-level access to the database, as well as the necessary runtime permissions.
6. Provide the following information to the system administrator who will install IBM Director Server:
  - Database name (if a database was created in step 5)
  - Node name (if IBM Director will connect remotely to DB2)
  - User ID and password, if necessary

## Microsoft Data Engine 2000 or SQL Server 2000 Desktop Engine

If you plan to use Microsoft Data Engine 2000 or SQL Server 2000 Desktop Engine, install the database application before installing IBM Director Server.

## Microsoft Jet 4.0

If you plan to install IBM Director Server on a server running Windows, you can use Microsoft Jet 4.0 as the IBM Director database. The Microsoft Jet 4.0 database engine is built into Windows 2000 and Windows Server 2003. When you install IBM Director Server, a single database file is created on the management server. This database has a maximum size of 2.14 gigabyte (GB). If you plan to manage more than 300 to 500 systems, you must use another database application.

## Microsoft SQL Server 2000

**Note:** If the management server and the database server are located in different domains, the following conditions apply:

- The IBM Director service account must be a domain account.
- There must be a trust relationship between the domains.

Complete the following tasks before installing IBM Director Server:

1. Install SQL Server, if you have not already done so.
2. Authorize the IBM Director service account to log on to SQL Server.
3. Complete one of the following tasks:
  - Assign the IBM Director service account Create Database permission in the master database. This allows the SQL Server database to be created *during* the installation of IBM Director. When the database is created during the IBM Director installation, the size of the database defaults to the larger of the following sizes:
    - The size of the model database
    - The default database size specified in the SQL Server configuration options
  - Create the SQL Server database. Either transfer ownership of the database to the IBM Director service account or give the IBM Director service account user-level access to the database, as well as the necessary runtime permissions.
4. Provide the following information to the system administrator who will install IBM Director Server:
  - Database name
  - Host name of the database server
  - Name for the Open Database Connectivity (ODBC) data source
  - User ID and password, if necessary

## Oracle Server

**Note:** IBM Director is certified to run with the Oracle Java Database Connectivity (JDBC) thin driver for use with Java Development Kit (JDK) 1.3 *only*. This JDBC driver does not require Oracle client software to be installed. However, it does require that Oracle Server be configured with a TCP/IP listener.

Complete the following tasks before installing IBM Director Server:

1. Install Oracle Server, if you have not done so already.
2. Make sure that the applicable Oracle JDBC thin driver is installed.

<b>For Oracle Server 8.1.7</b>	Version 9.0.1
<b>For Oracle Server 9.0</b>	Version 9.0.1
<b>For Oracle Server 9.2</b>	Version 9.2.0.3

You can download it from <http://www.otn.oracle.com/software/content.html>.

3. (Windows only) Make sure that the CLASSPATH statement points to the fully qualified name of the classes12.zip file that contains the Oracle JDBC driver.
4. Create the Oracle Server database.
5. Configure and start the Oracle TCP/IP listener.

6. Provide the following information to the system administrator who will install IBM Director Server:
  - Oracle administrator account ID and password
  - Oracle system identifier (SID)
  - Oracle TCP/IP listener port
  - TCP/IP host name of the database server

**Note:** The Oracle administrator account ID and password are used to create tablespaces and a role (TWG\_ROLE) and to assign a user ID and password. IBM Director *does not* save the Oracle administrator account ID and password.

## PostgreSQL

Complete the following tasks before installing IBM Director Server:

1. Install PostgreSQL, if you have not done so already. The IBM Redbooks publication *Implementing Systems Management Solutions Using IBM Director* (SG24-6188-01) contains tips and additional information that might be helpful. See “IBM Director documentation” on page xiv for more information.
2. Make sure that the JDBC driver is compatible with JDK 1.3.
3. Make sure that the PostgreSQL postmaster is running with the `-i` flag.
4. Create a PostgreSQL server ID for use with IBM Director.
5. Complete one of the following tasks:
  - Assign the PostgreSQL server ID that you created in step 4 Create Database permission. This allows the PostgreSQL database to be created *during* the installation of IBM Director Server.
  - Create the PostgreSQL database and either transfer ownership of the database to the PostgreSQL server ID that you created in step 4 or give the PostgreSQL server ID that you created in step 4 the necessary runtime permissions.
6. Provide the system administrator who will install IBM Director Server with the following information:
  - Database name (if the PostgreSQL database was created in step 5)
  - Host name of the database server
  - PostgreSQL IP listener port
  - User ID and password, if necessary

---

## IBM Director security

IBM Director offers several security features, including user-administration options that enable system administrators to specify user privileges, support for Secure Sockets Layer (SSL), and optional encryption of interprocess communication.

For information about how managed systems authenticate IBM Director Server, see Appendix A, “IBM Director Agent — IBM Director Server security,” on page 233

## IBM Director service account (Windows only)

Before installing IBM Director Server, create an operating-system user account with administrator privileges on the management server. This account is the *IBM Director service account*. The IBM Director Server service runs as this account, so consider selecting **Password never expires** when you create the account.

If you want to give Director group privileges to an entire domain group, the IBM Director service account should have domain administrator privileges. If the account only has local administrator privileges, you have to assign domain members to Director groups individually. If the IBM Director server account has domain administrator privileges, make sure to add the account to the local administrator group on the management server.

**Notes:**

1. It is a best practice to use the IBM Director service account *only* for IBM Director system administration.
2. Do not use either DirAdmin or DirSuper as the user ID for the IBM Director Service account.

## IBM Director user accounts

IBM Director user accounts are based upon the underlying operating-system accounts. When IBM Director Server is installed, two groups of IBM Director users are created automatically: administrators and super users. The two user groups have different levels of access to IBM Director:

### Administrator group

Members of the administrator group have general access to IBM Director, although the privileges available to the administrator group or an individual user can be restricted by a super user.

### Super-user group

Members of the super-user group can define the privileges available to the administrator group. Also, they can create and edit individual user accounts. The privileges available to members of the super-user group cannot be restricted.

The following table lists the operating-system specific names of the IBM Director user groups.

*Table 14. IBM Director user groups*

Operating system	Administrator group	Super-user group
i5/OS	QIBM_QDIR_ADMINISTRATOR	QIBM_QDIR_SUPER_ADM_PRIVILEGES
Linux	diradmin	dirsuper
Windows	DirAdmin	DirSuper

On i5/OS, the groups are not automatically populated. A user with security administrator authority must assign users to the appropriate groups

On Linux, the groups are not automatically populated. A user with root privileges must assign users to the appropriate groups.

On Windows, the IBM Director service account is automatically assigned to the super-user group (DirSuper). In addition, all operating-systems accounts with administrator privileges on the management server automatically can access IBM Director Console. Users with such operating-system accounts can access the same IBM Director privileges as members of the DirAdmin group.

## Secure Sockets Layer (SSL)

You can use SSL to protect data flowing between IBM Director Server and IBM Director Console.

IBM Director supports the following cipher suites:

- SSL\_RSA\_WITH\_RC4\_128\_MD5
- SSL\_RSA\_WITH\_RC4\_128\_SHA
- SSL\_RSA\_WITH\_DES\_CBC\_SHA
- SSL\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
- SSL\_DHE\_RSA\_WITH\_DES\_CBC\_SH
- SSL\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
- SSL\_DHE\_DSS\_WITH\_DES\_CBC\_SHA
- SSL\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA
- SSL\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5
- SSL\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA
- SSL\_RSA\_EXPORT\_WITH\_RC2\_CBC\_40\_MD5
- SSL\_DHE\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA
- SSL\_DHE\_DSS\_EXPORT\_WITH\_DES40\_CBC\_SHA
- SSL\_RSA\_WITH\_NULL\_MD5
- SSL\_RSA\_WITH\_NULL\_SHA
- SSL\_DH\_anon\_WITH\_RC4\_128\_MD5
- SSL\_DH\_anon\_WITH\_DES\_CBC\_SHA
- SSL\_DH\_anon\_WITH\_3DES\_EDE\_CBC\_SHA
- SSL\_DH\_anon\_EXPORT\_WITH\_RC4\_40\_MD5
- SSL\_DH\_anon\_EXPORT\_WITH\_DES40\_CBC\_SHA

See the documentation for the operating system on which you are running IBM Director to determine which cipher suites are supported by the operating system.

## Encryption

IBM Director contains a security feature that encrypts all data in interprocess communications, except for the transport-layer datagrams used during discovery. This encryption feature provides automatic key management and enables the user to select an encryption algorithm from the provided libraries:

- IBM Java Cryptography Extension (JCE)
- OpenSSL

JCE provides ciphers for all Java-based platforms, including i5/OS and Linux; OpenSSL provides ciphers for 32-bit Windows operating systems.

Encryption is disabled by default. To encrypt data transmitted between IBM Director Agent and IBM Director Server, you must enable encryption on both IBM Director Server and IBM Director Agent.

When you install IBM Director Server, you can select one of the following encryption algorithms:

- Data Encryption Standard (DES)
- Triple DES

IBM Director Server automatically generates a key, based on the encryption algorithm selected. IBM Director Server stores the key in memory and presents it to IBM Director Agent each time IBM Director Agent is started, using the Diffie-Hellman key exchange. This makes it unnecessary for a key to be stored on each managed system.

The following table outlines how data is transmitted between IBM Director Server and IBM Director Agent, depending on whether encryption is enabled.

*Table 15. Encryption state and data transmitted between IBM Director Server and IBM Director Agent*

	<b>IBM Director Agent (encryption enabled)</b>	<b>IBM Director Agent (encryption disabled)</b>
<b>IBM Director Server (encryption enabled)</b>	Encrypted	Unencrypted
<b>IBM Director Server (encryption disabled)</b>	No data transmission possible	Unencrypted

An exception to the matrix described in the table is the following scenario: There are two management servers. Encryption is disabled on one (server A) and enabled on the other (server B). Server A is authorized to manage server B, *and* server B is authorized to manage server A. Unencrypted transmissions sent by server A to server B are not rejected, despite the fact that server B had elected to encrypt all data transmissions. This occurs because server B, in its role as management server, is already communicating with server A (in its role as managed system) in plain text.

**Notes:**

1. Encryption is not supported on managed systems running NetWare, systems running 64-bit versions of Windows, or systems using SNA as a network protocol.
2. Neither out-of-band communications nor communication used by Internet tools, such as Telnet or File Transfer Protocol (FTP), are encrypted.
3. Enabling encryption imposes a performance penalty. Encrypting data packets and exchanging encryption keys has an effect on the speed with which IBM Director completes management operations. When either the management server or the managed systems are restarted, keys are regenerated and exchanged. Consequently, an unsecured managed system might appear to be unmanageable for a period of time.

## Web-based Access security

To use Web-based Access, a user must log in to an operating-system account on the local system. When the user is logged in, user privileges are based on operating-system privileges. Users with administrator authority can use Web-based Access to modify system settings, but users with user authority can view system settings only.



---

## Part 2. Installing IBM Director



---

## Chapter 4. Installing IBM Director Server

This chapter contains instructions for installing IBM Director Server. If you are upgrading IBM Director Server, go to Chapter 10, “Upgrading IBM Director Server,” on page 147.

**Important:** Before you install IBM Director Server, make sure that you have installed and configured the database application that you will use with IBM Director. See “Preparing the IBM Director database” on page 28 for more information.

---

### Preparing to install IBM Director Server on an xSeries server

Before you install IBM Director Server, make sure that the instance of IBM Director Agent running on the management server will be fully functional and able to send alerts to IBM Director Server. This might require installing service processor device drivers or the IBM LM78 and SMBus device drivers for Linux.

#### Service processor device drivers

If you plan to install IBM Director Server on an xSeries server that contains one of the following service processors, make sure that the service processor device driver has been installed:

- Advanced System Management processor
- Advanced System Management PCI Adapter
- Remote Supervisor Adapter
- Remote Supervisor Adapter II

If the device driver is not installed before you install IBM Director Server, the power indications provider might not be installed. This component monitors power supplies and generates alerts in the event of failure.

#### IBM LM78 and SMBus device drivers for Linux

If you plan to install IBM Director Server on an xSeries server running Linux, you might need to install either or both the LM78 and SMBus device drivers for Linux. These device drivers ensure that certain IBM Director tasks and functions work properly.

The following table contains information about these device drivers, when they need to be installed, and what they do.

*Table 16. Installing IBM Director Server: IBM LM78 and SMBus device drivers for Linux*

Device driver	When it is needed	What it does
LM78	If either of the following conditions apply: <ul style="list-style-type: none"><li>• The server is an xSeries 225, machine type 8647 server.</li><li>• The server contains an integrated systems management processor (ISMP).</li></ul>	The LM78 device driver ensures that IBM Director Server receives memory and processor Predictive Failure Analysis <sup>®</sup> (PFA) alerts.
SMBus	If the server does not contain one of the following service processors: <ul style="list-style-type: none"><li>• IPMI baseboard management controller</li><li>• Remote Supervisor Adapter</li><li>• Remote Supervisor Adapter II</li></ul>	The SMBus device driver ensures that the Management Processor Assistant tasks and System Health Monitoring function properly.

## Downloading and installing the LM78 and SMBus device drivers

You must perform the following steps to install either the IBM LM78 or SMBus device driver:

1. Download the TAR.GZ file that contains the source Red Hat Package Manager (RPM™) file from the IBM Web site
2. Build the binary RPM file
3. Install the binary RPM file on the system on which you will install IBM Director Server

### Downloading the IBM LM78 and SMBus device drivers

The following table provides information about the TAR.GZ files that contain the source RPM files for the LM78 and SMBus device drivers.

Table 17. Installing IBM Director Server: Source files for the LM78 and SMBus device drivers

Device driver	Operating system	File name
LM78	Red Hat Linux VMware ESX Server	dir4.20_lm78_redhatlinux.tar.gz
	SUSE LINUX	dir4.20_lm78_suselinux.tar.gz
SMBus	Red Hat Linux VMware ESX Server	dir4.20_smb_redhatlinux.tar.gz
	SUSE LINUX	dir4.20_smb_suselinux.tar.gz

You can download the files from the IBM Systems Management Software: Download/Electronic Support page at [http://www.ibm.com/pc/us/eserver/xseries/systems\\_management/dwnl.html](http://www.ibm.com/pc/us/eserver/xseries/systems_management/dwnl.html).

### Building the binary RPM file

You must build the binary RPM file on a system with the same kernel version and hardware configuration as the system on which you will install IBM Director Server. Make sure that the hardware configuration is similar in regard to the number of processors.

Complete the following steps to build either the LM78 or SMBus device driver:

1. Configure a system with the appropriate operating system and hardware configuration. Verify that the Linux kernel source is installed and properly configured.
2. Decompress the TAR.GZ file that contains the source RPM file.
3. To install the source RPM file, from a command prompt, type one of the following commands and press Enter:

<b>Red Hat Linux and VMware ESX Server</b>	<code>rpm -ivh driver-src-redhat-4.20-1.i386.rpm</code>
<b>SUSE LINUX</b>	<code>rpm -ivh driver-src-suse-4.20-1.i386.rpm</code>

where *driver* is either *ibmlm78* or *ibmsmb*. This creates a binary RPM file in either the `/usr/local/ibmlm78` or the `/usr/local/smbus` directory, depending on which source RPM file you installed.

## Installing the IBM LM78 or SMBus device driver

**Note:** In this procedure, *driver* is one of the following strings:

---

<b>For the IBM LM78 device driver</b>	ibmlm78
<b>For the IBM SMBus device driver</b>	ibmsmb

---

Complete the following steps to install either the IBM LM78 or SMBus device driver:

1. If you built the binary RPM file on another server, create a `/usr/local/driver` directory on the server where you will install IBM Director Server. Copy the binary RPM file to that directory.
2. Change to the `/usr/local/driver` directory.
3. To install the device driver, from a command prompt, type the following command and press Enter:

```
rpm -ivh driver-4.20-1.i386.rpm
```

Issuing the command accomplishes the following tasks:

- Uncompresses and untars the archive into the `/usr/local/driver` directory
- Copies the device driver, shared library, and all configuration files to their appropriate locations
- Loads the device driver

---

## Installing IBM Director Server on i5/OS

See the IBM Virtualization Engine documentation for instructions for installing IBM Director Server on i5/OS. The IBM Virtualization Engine documentation is part of the IBM @server Information Center at <http://www.ibm.com/servers/library/infocenter>.

After you have installed IBM Director Server, complete the following steps to enable encryption:

1. Stop IBM Director Server.
2. Using an ASCII text editor or the i5/OS Edit File (EDTF) command, open the `/QIBM/ProdData/Java400/jdk13/lib/security/java.security` file.
3. Uncomment the following line by removing the hash (#) at the beginning of the line:

```
security.provider.3=com.ibm.crypto.provider.IBMJCE
```

4. Restart IBM Director Server.

---

## Installing IBM Director Server on Linux

This section provides instructions for installing IBM Director Server. When you install IBM Director Server, IBM Director Console and IBM Director Agent are installed automatically. During the installation process, you can install the Server Plus Pack extensions and several IBM Director Agent features. You also can enable encryption.

**Notes:**

1. Before you install IBM Director Server on Red Hat Enterprise Linux AS, version 3.0, for Intel x86, make sure that the following RPM file is installed:  
`compat-libstdc++-7.3-2.96.122.i386.rpm`

2. (Management server running SUSE LINUX only) If you plan to install Active PCI Manager and want to run the task against the management server, make sure that you have installed the necessary prerequisites. For more information, see Table 20, “IBM Active PCI Software necessary to run Active PCI Manager,” and Table 21, “Network adapter device drivers necessary to run the Fault Tolerant Management Interface,” on page 134.

Complete the following steps to install IBM Director Server on Linux:

1. Insert the *IBM Director 4.20* CD into the CD-ROM drive.
2. If the CD does not automount, go to step 3. If the CD automounts, type the following command and press Enter:

```
umount /mnt/cdrom
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

3. Type the following command and press Enter:

```
mount -t iso9660 -o map=off /dev/cdrom /mnt/cdrom
```

where *dev/cdrom* is the specific device file for the CD-ROM block device and *mnt/cdrom* is the mount point of the CD-ROM drive.

4. Change to the directory where the installation script is located. Type the following command and press Enter:

```
cd /mnt/cdrom/director/server/linux/i386/
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

5. If you want to customize the installation, go to step 6. If you want to accept the default settings for the installation, type the following command and press Enter:

```
./dirinstall
```

Go to step 10.

6. To customize the installation, copy the installation script to a local directory. Type the following command and press Enter:

```
cp dirinstall /directory/dirinstall
```

where *directory* is the local directory.

7. Open an ASCII text editor and modify the “User configuration” section of the *dirinstall* script. This file is fully commented.

You can specify the location of the RPM files, select the IBM Director extensions and features that you want to install, and select log file options.

8. Save the modified installation script.
9. To install IBM Director, type the following command and press Enter:

```
/directory/dirinstall
```

where *directory* is the local directory to which you copied the installation script.

10. Prepare to configure your database application for use with IBM Director.

If the database application is	Go to
IBM DB2 Universal Database	Step 11 on page 43
Oracle Server	Step 13 on page 43
PostgreSQL	Step 15 on page 43
Configure later (database disabled)	Step 18 on page 43

11. (DB2 only) Create a `/etc/TWGserver/setup_env` file. Add the following statement to the file:

```
. /home/db2inst1/sqllib/db2profile
```

where `home/db2inst1` is the directory where DB2 is installed. This statement sets up the DB2 environment.

12. Set the `setup_env` file attributes to read-execute. Go to step 18.
13. (Oracle only) Create a `/etc/TWGserver/setup_env` file. Add the following statements to the file:

```
CLASSPATH=path/classes12.zip  
export CLASSPATH
```

where `path` is the path of the `classes12.zip` file that contains the Oracle JDBC driver.

14. Set the `setup_env` file attributes to read-execute. Go to step 18.
15. (PostgreSQL only) If the PostgreSQL JDBC driver is named `postgresql.jar`, go to step 16. Otherwise, you must create a symbolic link. From a command prompt, type the following command and press Enter:

```
ln -s realname path/postgresql.jar
```

where `realname` is the fully qualified name of the PostgreSQL JDBC driver, for example, `/opt/postgres/lib/jdbc7.1-2.jar`, and `path` is the path of the symbolic link, for example, `/opt/postgres/lib/`.

16. Create a `/etc/TWGserver/setup_env` file. Add the following statement to the file:

```
export CLASSPATH=path/postgresql.jar
```

where `path` is the path of the PostgreSQL JDBC driver, for example, `/opt/postgres/lib`.

**Note:** If you created a symbolic link in step 15, `path` is the path of the symbolic link.

17. Set the `setup_env` file attributes to read-execute.
18. To configure the database for use with IBM Director, type the following command and press Enter:

```
/opt/IBM/director/bin/cfgdb
```

Follow the instructions on the screen.

19. To enable encryption or change security settings, type the following command and press Enter:

```
/opt/IBM/director/bin/cfgsecurity
```

20. To start IBM Director, type the following command and press Enter:

```
/opt/IBM/director/bin/twgstart
```

21. To unmount the CD-ROM drive, complete the following steps:

- a. Type `cd /` and press Enter.
- b. Type the following command and press Enter:

```
umount mnt/cdrom
```

where `mnt/cdrom` is the mount point of the CD-ROM drive.

22. Remove the *IBM Director 4.20* CD from the CD-ROM drive.

To enable SNMP Access and Trap Forwarding, install and configure Net-SNMP, version 5.0.9. See “Enabling SNMP Access and Trap Forwarding for Linux” on page 198.

For instructions for installing IBM Director Software Distribution (Premium Edition) and the Rack Manager component, see “Completing the Rack Manager installation on the management server” on page 131 and “Installing Software Distribution (Premium Edition)” on page 132

---

## Installing IBM Director Server on Windows

This section provides instructions for installing IBM Director Server. When you install IBM Director Server, the InstallShield wizard also automatically installs IBM Director Console and IBM Director Agent. During the installation process, you can install the Server Plus Pack extensions and the optional IBM Director Agent features. You also can enable encryption.

**Note:** If you plan to install Active PCI Manager and want to run the task against the management server, make sure that you have installed the necessary prerequisites. For more information, see Table 20, “IBM Active PCI Software necessary to run Active PCI Manager,” and Table 21, “Network adapter device drivers necessary to run the Fault Tolerant Management Interface,” on page 134.

Complete the following steps to install IBM Director Server:

1. Using an account with either local or domain administrative privileges, log on to the operating system.
2. Insert the *IBM Director 4.20* CD into the CD-ROM drive.
3. If the installation program starts automatically and the InstallShield wizard starts, go to step 5. Otherwise, click **Start** → **Run**.
4. In the **Open** field, type the following command and press Enter:  
`e:\setup.exe`

where *e* is the drive letter of the CD-ROM drive. The installation program starts, and the “IBM Director” window opens.

5. Click **Install IBM Director**. The “IBM Director Installation” window opens.
6. Click **IBM Director Server installation**. The InstallShield wizard starts, and the “Welcome to the InstallShield Wizard” window opens.
7. Click **Next**. The “License Agreement” window opens.
8. Click **I accept the terms in the license agreement**; then, click **Next**. The “Server Plus Pack” window opens.



Figure 4. Installing IBM Director Server on Windows: “Server Plus Pack” window

9. Click **Next**. The “Feature and installation directory selection” window opens.

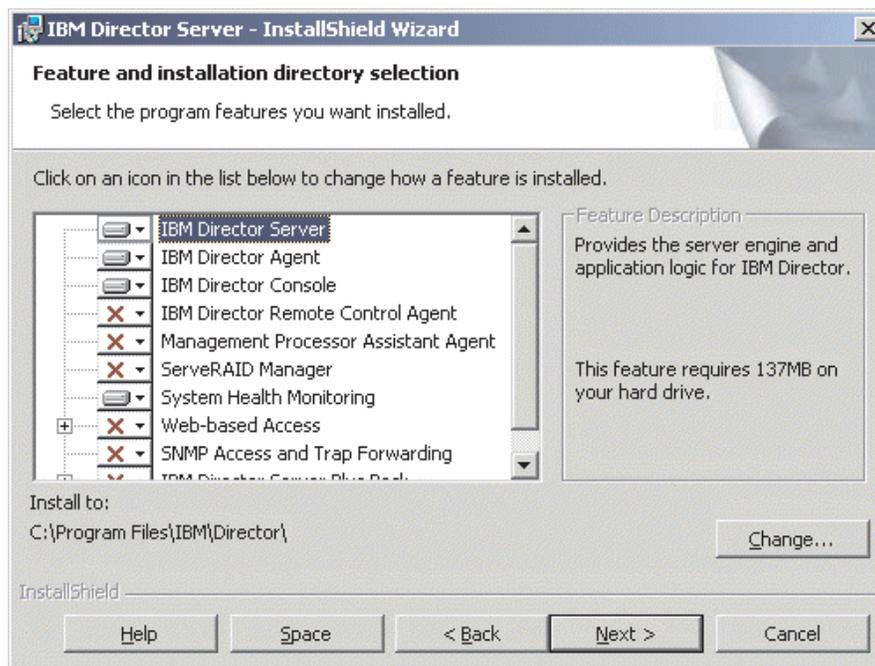


Figure 5. Installing IBM Director Server on Windows: “Feature and installation directory selection” window

IBM Director Server, IBM Director Agent, IBM Director Console, and System Health Monitoring are selected automatically for installation; a hard disk drive icon  is displayed to the left of each component.  is displayed to the left of the optional features that are not selected by default.

10. Select the IBM Director Agent features that you want to install:

**IBM Director Remote Control Agent**

Enables a system administrator to perform remote desktop functions on the management server

**Management Processor Assistant Agent**

(IBM xSeries and Netfinity servers only) Enables communication with service processors that are present in the management server

**ServeRAID Manager**

Manages and monitors IBM ServeRAID adapters and integrated SCSI controllers with RAID capabilities that are present in the management server

**System Health Monitoring**

Monitors the status of hardware components that are present in the management server, produces and relays hardware alerts, and facilitates upward integration

**Web-based Access**

Enables a system administrator to access the management-server data through a Web browser or the Microsoft Management Console (MMC)

**SNMP Access and Trap Forwarding**

Enables access to management-server data and alerts through SNMP

To select a feature, click  to the left of the feature name. A menu opens. To select the feature, click either **This feature will be installed on local hard drive** or **This feature, and all subfeatures, will be installed on local hard drive**.

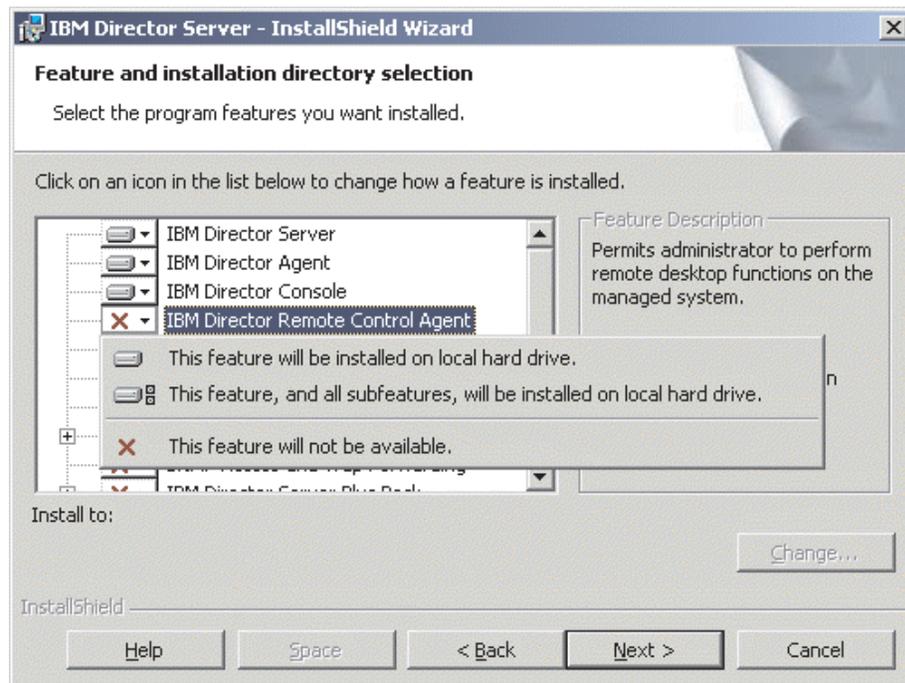


Figure 6. Installing IBM Director Server on Windows: “Features and installation directory selection” window

11. Select the Server Plus Pack extensions that you want to install:

**Capacity Manager**

Tracks system resource utilization, identifies bottlenecks, and provides performance information

**Rack Manager**

Manages IBM servers, storage devices, and other components in an IBM enclosure

**Active PCI Manager**

Manages PCI and PCI-X adapters in managed systems

**Software Rejuvenation**

Schedules restarts of managed systems

**System Availability**

Determines availability of managed systems and provides statistical data

To select the complete Server Plus Pack, click the icon to the left of **IBM Director Server Plus Pack**; then, click **This feature, and all subfeatures, will be installed on local hard drive**. Otherwise, select the Server Plus Pack extensions individually.

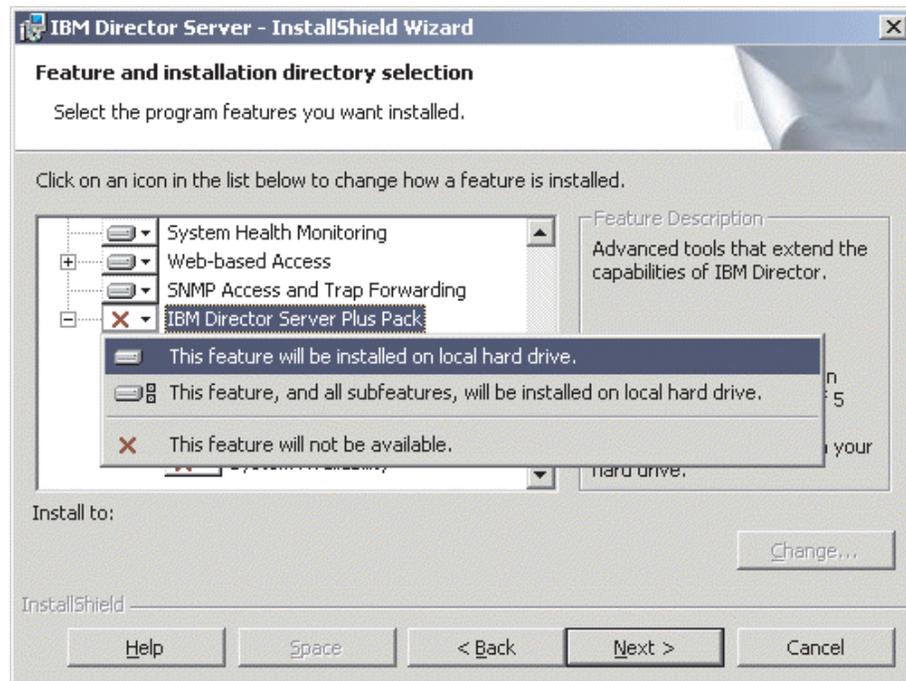


Figure 7. Installing IBM Director Server on Windows: Installing the Server Plus Pack

**Notes:**

- a. Until you install the Server Plus Pack extensions on the managed systems, you can run the Server Plus Pack tasks only against the management server.
- b. You cannot run the Rack Manager task against the management server until the Rack Manager component, which is on the *IBM Director Server Plus Pack* CD, is installed on the management server.

12. Click **Next**. The “IBM Director service account information” window opens. For more information, see “IBM Director service account (Windows only)” on page 32.



The screenshot shows a Windows-style dialog box titled "IBM Director Server - InstallShield Wizard". The main heading is "IBM Director service account information". Below the heading, it says "Provide the following information about the IBM Director service account." There are four text input fields: "Local computer name or domain:", "User name:", "Password:", and "Confirm password:". At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel". The "Next >" button is highlighted with a mouse cursor.

Figure 8. Installing IBM Director Server on Windows: “IBM Director service account information” window

13. Provide information about the IBM Director service account:
  - a. In the **Local computer name or domain** field, type the computer name of the IBM Director service account. If the service account is a domain account, type the domain.
  - b. In the **User Name** field, type the user ID for the IBM Director service account.
  - c. In the **Password** and **Confirm Password** fields, type the password for the IBM Director service account.

**Note:** The information must correspond to a Windows account with administrator privileges on the management server. Otherwise, the installation will fail.

14. Click **Next**. The “Encryption settings” window opens.

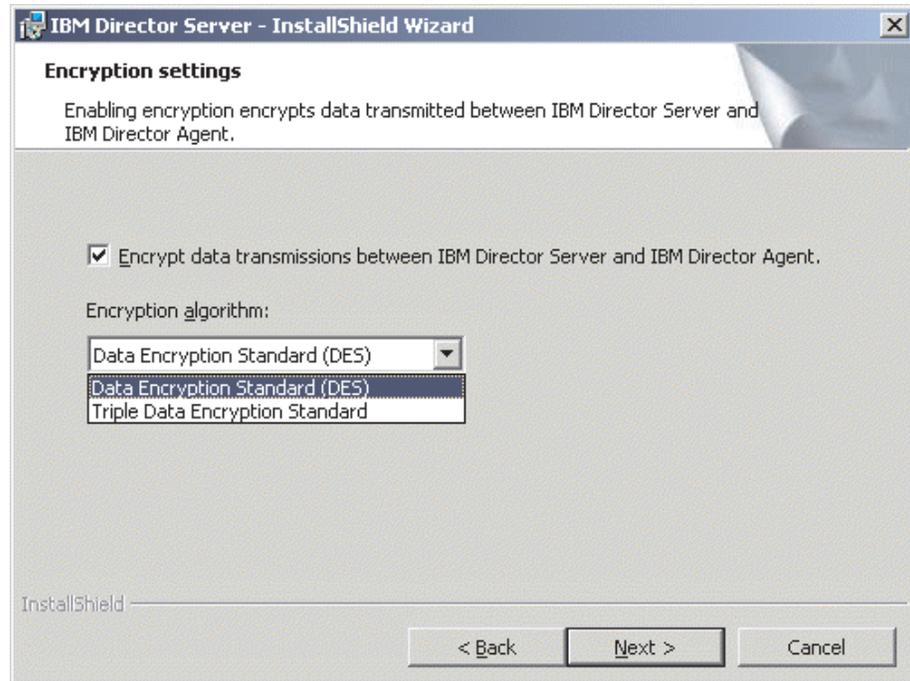


Figure 9. Installing IBM Director Server on Windows: “Encryption settings” window

15. To encrypt data that is transmitted between IBM Director Server and IBM Director Agent, select the **Encrypt data transmissions between IBM Director Server and IBM Director Agent** check box; then, select the encryption algorithm.
16. Click **Next**. The “Software-distribution settings” window opens.

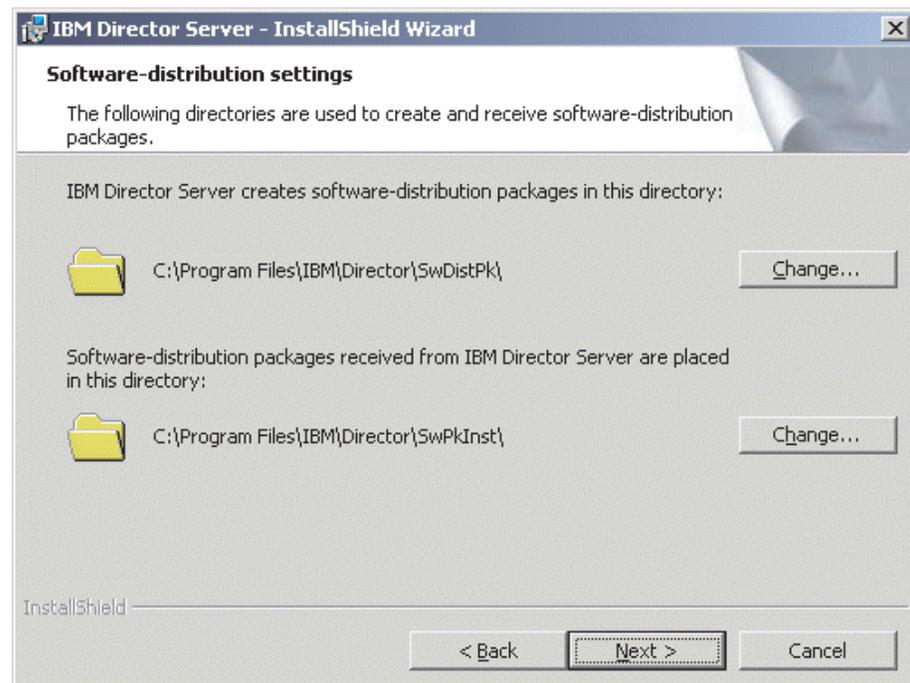


Figure 10. Installing IBM Director Server on Windows: “Software-distribution settings” window

17. To select an alternative location for where IBM Director Server creates software-distribution packages, click **Change** and select another directory.  
To select an alternative location for where software-distribution packages that are received from IBM Director Server are placed, click **Change** and select another directory.
18. Click **Next**. If you did not select to install the Web-based Access feature, the “Ready to Install the Program” window opens; go to step 20. Otherwise, the “Web-based Access information” window opens.

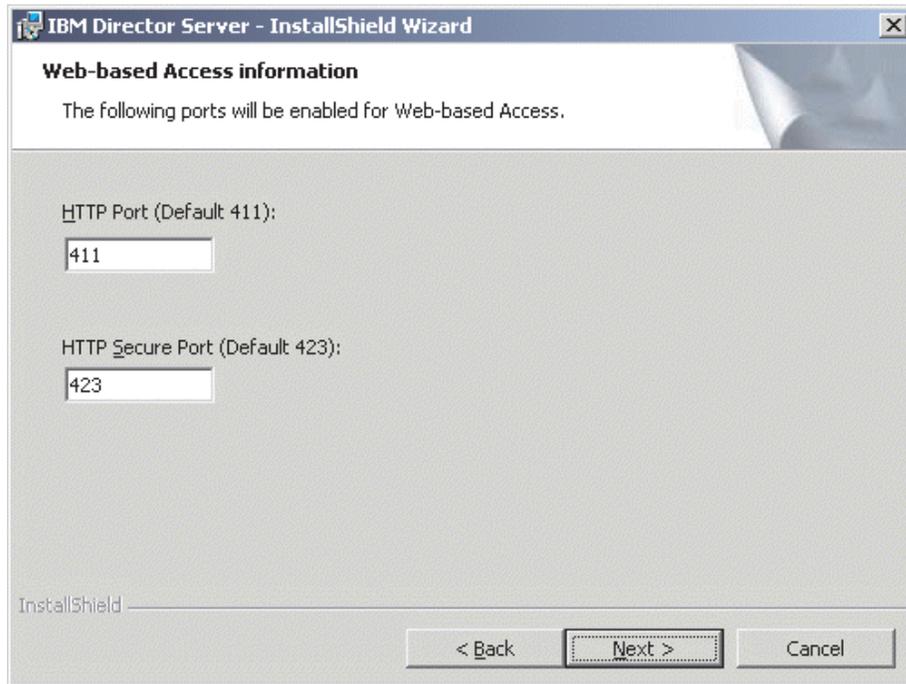


Figure 11. Installing IBM Director Server on Windows: “Web-based Access information” window

19. Change the default HTTP ports (if necessary); then, click **Next**. The “Ready to Install the Program” window opens.
20. Click **Install**. The “Installing IBM Director Server” window opens. The progress of the installation is displayed in the **Status** field. When the installation is completed, the “Network driver configuration” window opens.

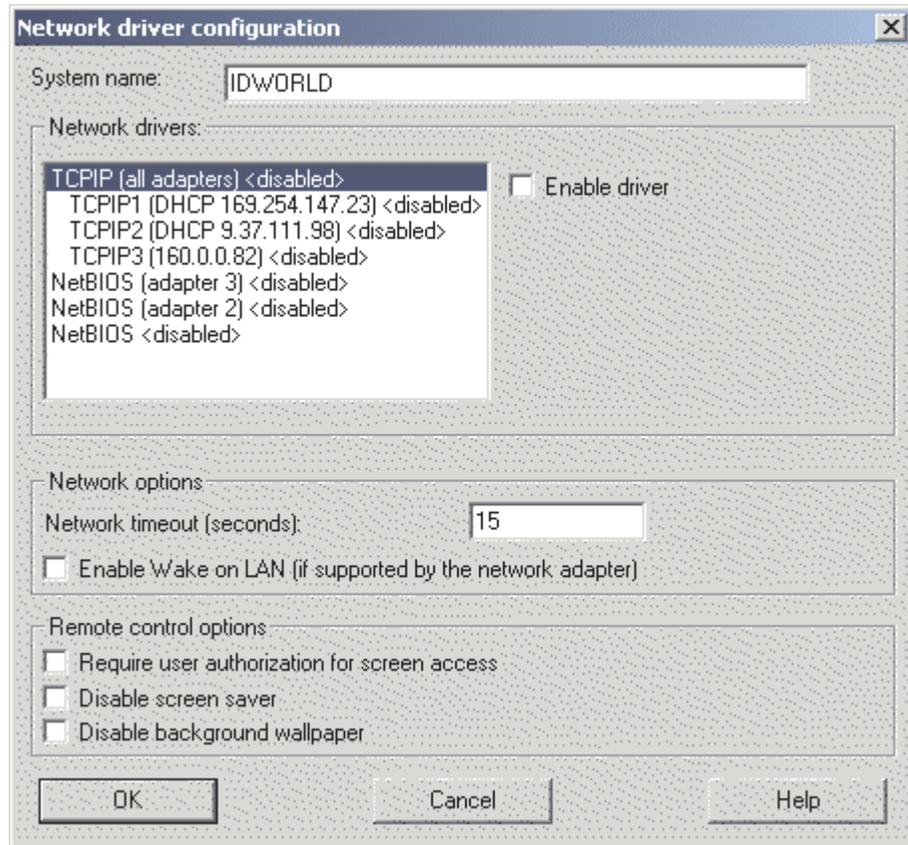


Figure 12. Installing IBM Director Server on Windows: “Network driver configuration” window

21. In the **System name** field, type the name that you want to be displayed in IBM Director Console. By default, this is the NetBIOS name of the management server.
22. Define the communications protocols to use for communication between IBM Director Server and IBM Director Agent.
  - a. In the **Network drivers** field, TCPIP (all adapters) is enabled by default. To enable another protocol, select the protocol and then select the **Enable driver** check box.

**Note:** If you disable TCPIP (all adapters) and enable an individual device driver on a system with multiple network adapters, IBM Director Server will receive *only* those data packets addressed to the individual adapter.

- b. In the **Network timeout** field, type the number of seconds that IBM Director Server waits for a response from IBM Director Agent. By default, this is set to 15 seconds.
- c. Select the **Enable Wake on LAN** check box if the network adapter supports the Wake on LAN<sup>®</sup> feature.

**Note:** To determine whether your server supports the Wake on LAN feature, see your server documentation.

23. If you selected to install the IBM Director Remote Control Agent, the following options are available:

**Require user authorization for system access**

Select this check box to request authorization from the local user before controlling the management server remotely.

**Disable screen saver**

Select this check box to disable the screen saver on the management server when it is controlled remotely.

**Disable background wallpaper**

Select this check box to disable desktop wallpaper on the management server when it is controlled remotely. You might want to disable the wallpaper because complicated backgrounds slow down remote control and increase network traffic.

24. Click **OK**. The “IBM Director database configuration” window opens.

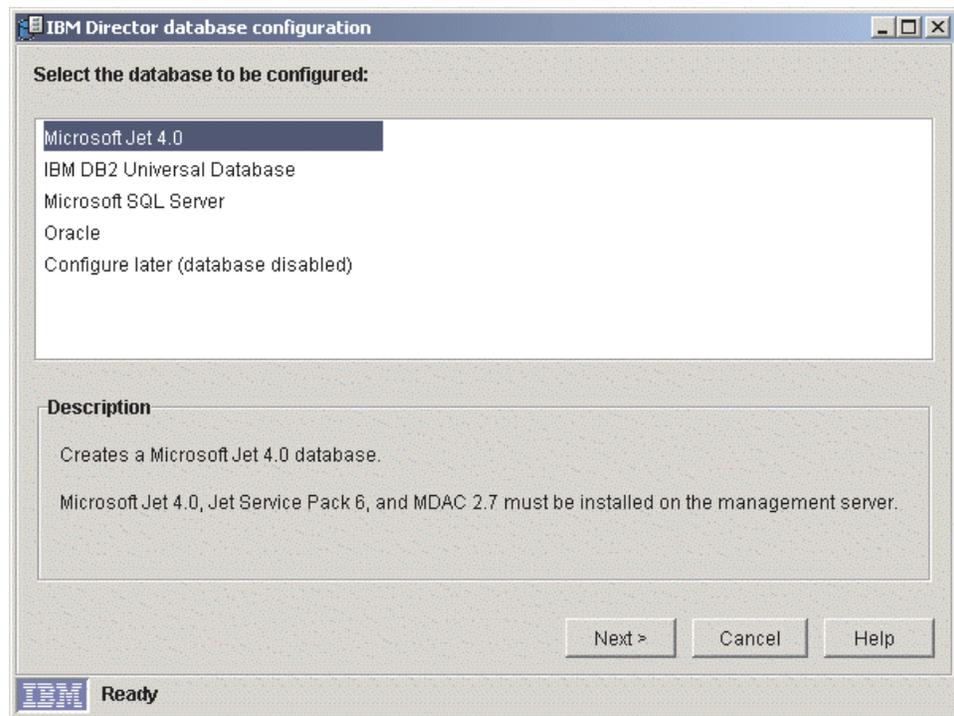


Figure 13. Installing IBM Director Server: “IBM Director database configuration” window

25. Click the database application that you want to use with IBM Director. You have the following options:

**Microsoft Jet 4.0**

Creates a Microsoft Jet 4.0 database. Microsoft Jet 4.0, Jet Service Pack 8, and MDAC 2.8 must be installed on the management server.

**IBM DB2 Universal Database**

Creates a DB2 database. DB2 Administration Client must be installed on the management server. IBM DB2 Universal Database must be installed and configured on a system in you network.

**Microsoft SQL Server**

Creates a Microsoft SQL Server database. Microsoft SQL Server must be installed and configured on a system in your network.

### Oracle

Configures an Oracle database. Oracle Server must be installed and configured on a system in your network.

### Configure later (database disabled)

IBM Director will be installed without a database. Tasks requiring a database will be absent or not functional.

26. Click **Next** and begin configuring the IBM Director database.

If you selected	Go to
Microsoft Jet 4.0	Step 32 on page 56
IBM DB2 Universal Database	Step 27
Microsoft SQL Server	Step 29 on page 54
Oracle	Step 30 on page 55
Configure later (database disabled)	Step 32 on page 56

27. The “IBM Director DB2 Universal Database configuration” window opens. Type information in the following entry fields:

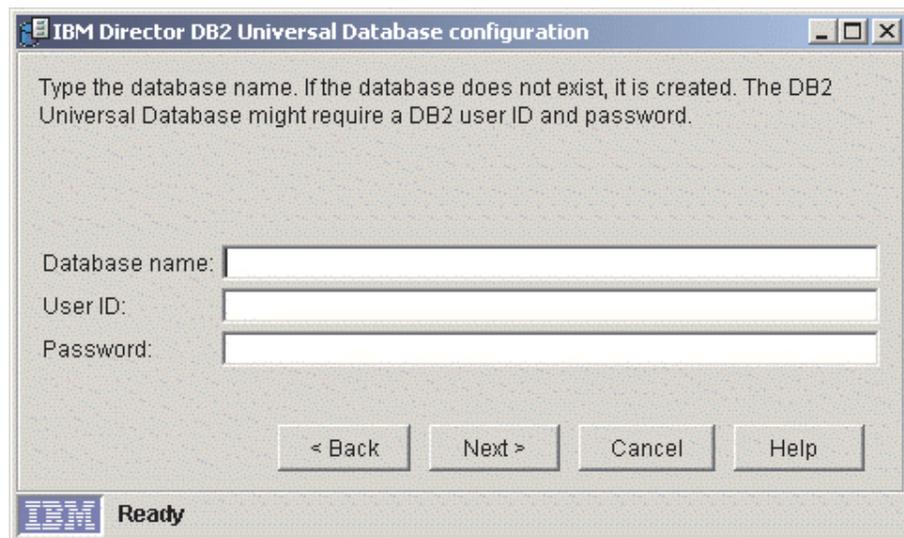


Figure 14. Installing IBM Director Server: “IBM Director DB2 Universal Database configuration” window

- a. In the **Database name** field, type the name of the database. If it does not exist, it will be created.
  - b. In the **User ID** field, type a valid DB2 user ID, if required.
  - c. In the **Password** field, type the password for the DB2 user ID, if required.
28. Click **Next**. The second “IBM Director DB2 Universal Database configuration” window opens.



Figure 15. Installing IBM Director Server: “IBM Director DB2 Universal Database configuration” window

In the **DB2 node name** field, select the location of the DB2 database. Then, click **OK** and go to step 32 on page 56.

29. The “IBM Director Microsoft SQL Server database configuration” window opens.

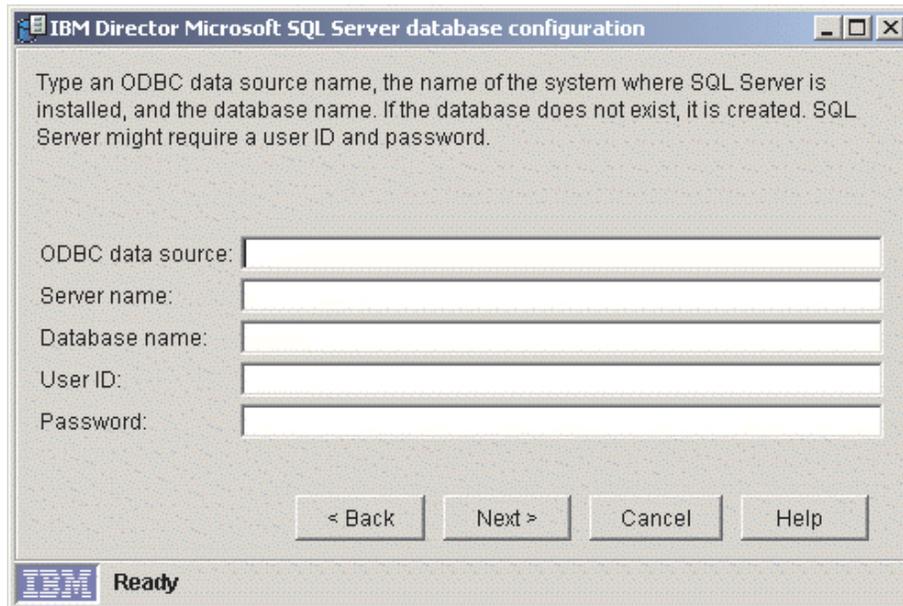


Figure 16. Installing IBM Director Server: “IBM Director Microsoft SQL Server database configuration” window

Type information in the following entry fields:

- a. In the **ODBC data source** field, type the name of the ODBC data source. If it does not exist, it will be created.
- b. In the **Server name** field, type the name of the server where SQL Server is installed.
- c. In the **Database name** field, type name of the database. If it does not exist, it will be created.
- d. In the **User ID** field, type a valid SQL Server user ID, if required.
- e. In the **Password** field, type the password for the SQL Server user ID, if required.

Click **Next**. Go to step 32 on page 56.

30. The “IBM Director Oracle database configuration” window opens.

Type the Oracle TCP/IP listener port, the host name of the system where Oracle is installed, and the Oracle System Identifier (SID). Oracle Server requires a user ID and password. The Oracle administrator account credentials are needed to create and configure the user ID and tablespaces.

Oracle TCP/IP listener port:

Oracle host name:

Oracle System Identifier (SID):

User ID:

Password:

Confirm password:

Oracle administrator account:

Oracle administrator password:

< Back   Next >   Cancel   Help

IBM Ready

Figure 17. Installing IBM Director Server: “IBM Director Oracle database configuration” window

Type information in the following entry fields:

- a. In the **Oracle TCP/IP listener port** field, type the number of the port that is used by the Oracle TCP/IP listener.
  - b. In the **Oracle host name** field, type the TCP/IP host name of the database server.
  - c. In the **Oracle System Identifier (SID)** field, type the Oracle system identifier (SID).
  - d. In the **User ID** field, type a valid Oracle user ID. If it does not exist, it is created. By default, this user ID is assigned to the IBM Director tablespace.
  - e. In the **Password** and **Confirm password** fields, type the password that is associated with the user ID that you typed in step 30d.
  - f. In the **Oracle administrator account** field, type a valid Oracle administrator account user ID.
  - g. In the **Oracle administrator password** field, type the password that is associated with the user ID that you typed in step 30f.
31. Click **Next**. The second “IBM Director Oracle database configuration” window opens.

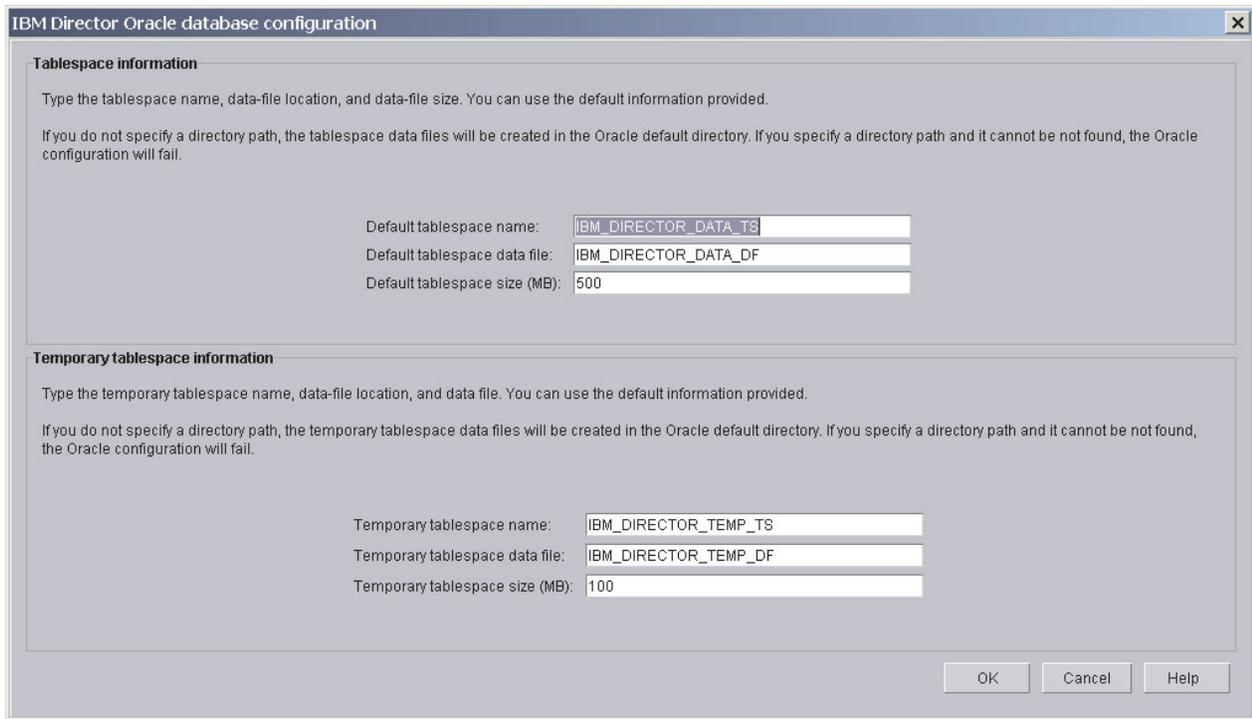


Figure 18. Installing IBM Director Server: “IBM Director Oracle database configuration” window

Type information in the following entry fields:

- a. In the **Default tablespace name** field, type a tablespace name.
  - b. In the **Default tablespace data file** field, type the name of the tablespace data file. If you do not specify the directory path, the tablespace data file will be created in the Oracle Server default directory. If you specify an invalid directory path, the database configuration will fail.
  - c. In the **Default tablespace size (MB)** field, type the size of the tablespace in MB.
  - d. In the **Temporary tablespace name** field, type a name for the temporary tablespace.
  - e. In the **Temporary tablespace data file** field, type the name of the temporary tablespace data file. If you do not specify the directory path, the tablespace data file will be created in the Oracle Server default directory. If you specify an invalid directory path, the database configuration will fail.
  - f. In the **Temporary tablespace size (MB)** field, type the size of the temporary tablespace in MB.
32. Click **OK**. The status bar displays the progress of the installation. When the installation is completed, the “InstallShield Wizard Completed” window opens.
  33. Click **Finish**. A window opens, asking you if you want to restart the server.
  34. Remove the *IBM Director 4.20* CD from the CD-ROM drive.
  35. Click **Yes** to restart the server.

For instructions for installing IBM Director Software Distribution (Premium Edition) and the Rack Manager component, see “Completing the Rack Manager installation on the management server” on page 131 and “Installing Software Distribution (Premium Edition)” on page 132

---

## Chapter 5. Installing IBM Director Console

This chapter contains instructions for installing IBM Director Console. If you are upgrading IBM Director Console, go to Chapter 11, “Upgrading IBM Director Console,” on page 161.

---

### Installing IBM Director Console on Linux

**Notes:**

1. IBM Director Console is not supported on the Gnome desktop environment.
2. Before you install IBM Director Console on Red Hat Enterprise Linux AS, version 3.0, for Intel x86, make sure that the following RPM file is installed:  
compat-libstdc++-7.3-2.96.122.i386.rpm

Complete the following steps to install IBM Director Console on Linux:

1. Insert the *IBM Director 4.20* CD into the CD-ROM drive.
2. If the CD does not automount, go to step 3. If the CD automounts, type the following command and press Enter:

```
umount /mnt/cdrom
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

3. Type the following command and press Enter:

```
mount -t iso9660 -o map=off /dev/cdrom /mnt/cdrom
```

where *dev/cdrom* is the specific device file for the CD-ROM block device and *mnt/cdrom* is mount point of the CD-ROM drive.

4. Change to the directory where the installation script is located. Type the following command and press Enter:

```
cd /mnt/cdrom/director/console/linux/i386/
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

5. If you want to customize the installation, go to step 6. If you want to accept the default settings for the installation, type the following command and press Enter:

```
./dirinstall
```

Go to step 10 on page 58.

6. To customize the installation, copy the installation script to a local directory. Type the following command and press Enter:

```
cp dirinstall /directory/dirinstall
```

where *directory* is the local directory.

7. Open an ASCII text editor and modify the “User configuration” section of the *dirinstall* script. This file is fully commented.

You can specify the location of the RPM files, select the IBM Director extensions and features that you want to install, and select log file options.

8. Save the modified installation script.

9. To install IBM Director, type the following command and press Enter:

```
/directory/dirinstall
```

where *directory* is the local directory to which you copied the installation script.

10. To unmount the CD-ROM drive, complete the following steps:

- a. Type `cd /` and press Enter.
- b. Type the following command and press Enter:

```
umount /mnt/cdrom
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

11. Remove the *IBM Director 4.20* CD from the CD-ROM drive.

---

## Installing IBM Director Console on Windows

This section describes how to install IBM Director Console. You can install IBM Director Console on any system from which you want to remotely access IBM Director Server.

This section provides instructions for installing IBM Director Console using the InstallShield wizard. The wizard can be used in a standard interactive mode, or you can perform an unattended installation using a response file to provide answers to the questions that the wizard poses.

**Note:** Early versions of Active PCI Manager are not compatible with IBM Director. Before you install IBM Director, make sure that you have uninstalled any Active PCI Manager, versions 1.0, 1.1, and 3.1.1, components.

### Installing IBM Director Console using the InstallShield wizard

Complete the following steps to install IBM Director Console on Windows:

1. Insert the *IBM Director 4.20* CD into the CD-ROM drive.
2. If the installation program starts automatically and the InstallShield wizard starts, go to step 4. Otherwise, click **Start** → **Run**.
3. In the **Open** field, type the following command and press Enter:

```
e:\setup.exe
```

where *e* is the drive letter of the CD-ROM drive. The installation program starts, and the “IBM Director” window opens.

4. Click **Install IBM Director**. The “IBM Director Installation” window opens.
5. Click **IBM Director Console installation**. The “Welcome to the InstallShield Wizard” window opens.
6. Click **Next**. The “License Agreement” window opens.
7. Click **I accept the terms in the license agreement**; then, click **Next**. The “Server Plus Pack” window opens.



Figure 19. Installing IBM Director Console: “Server Plus Pack” window

8. Click **Next**. The “Feature and installation directory selection” window opens.

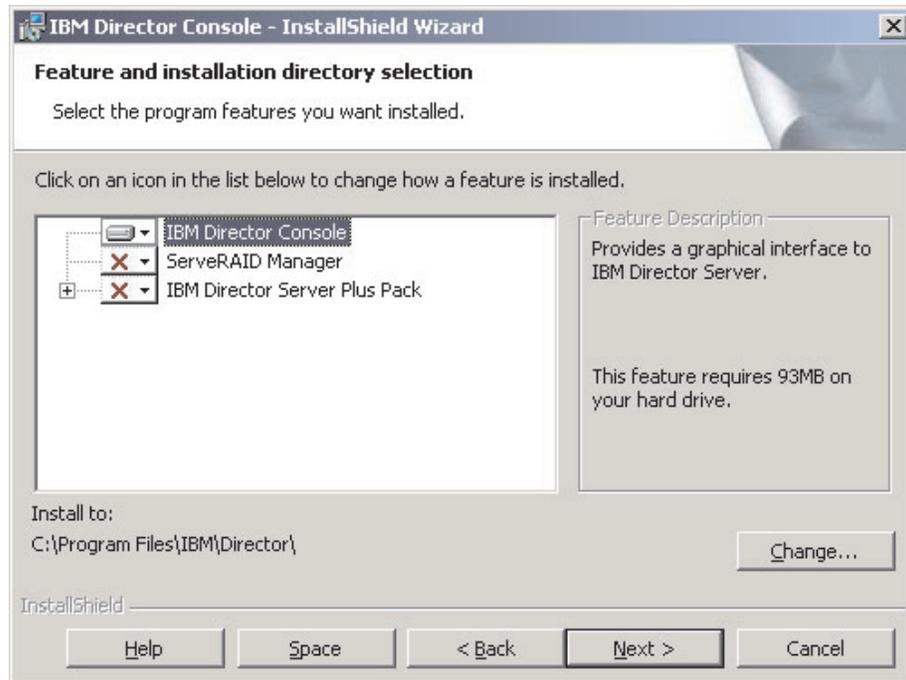


Figure 20. Installing IBM Director Console: “Feature and destination directory selection” window

IBM Director Console is selected automatically for installation; a hard disk drive icon  is displayed to its left.  is displayed to the left of the optional feature, ServeRAID Manager.

- To select ServeRAID Manager, a feature that manages and monitors IBM ServeRAID adapters, click  to the left of the feature name. A menu opens.

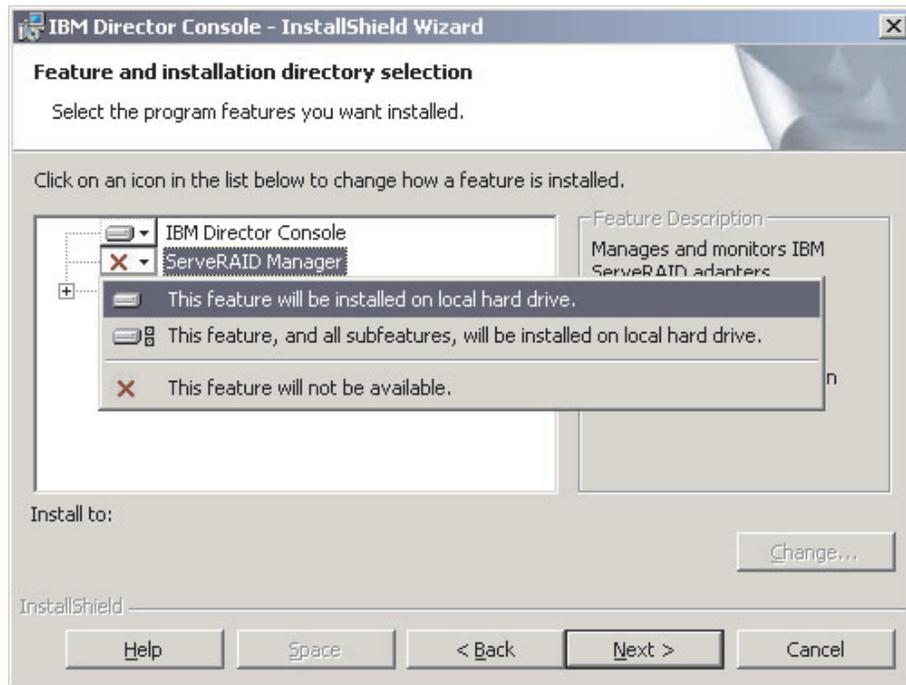


Figure 21. Installing IBM Director Console: Installing ServeRAID Manager

Click **This feature will be installed on local hard drive.**

- Select the Server Plus Pack extensions that you want to install:

**Capacity Manager**

Tracks system resource utilization, identifies bottlenecks, and provides performance information

**Rack Manager**

Manages IBM servers, storage devices, and other components in an IBM enclosure

**Active PCI Manager**

Manages PCI and PCI-X adapters in managed systems

**Software Rejuvenation**

Schedules restarts of managed systems

**System Availability**

Determines availability of managed systems and provides statistical data

To select the complete Server Plus Pack, click the icon to the left of **IBM Director Server Plus Pack**; then, click **This feature, and all subfeatures, will be installed on local hard drive.** Otherwise, select the Server Plus Pack extensions individually.

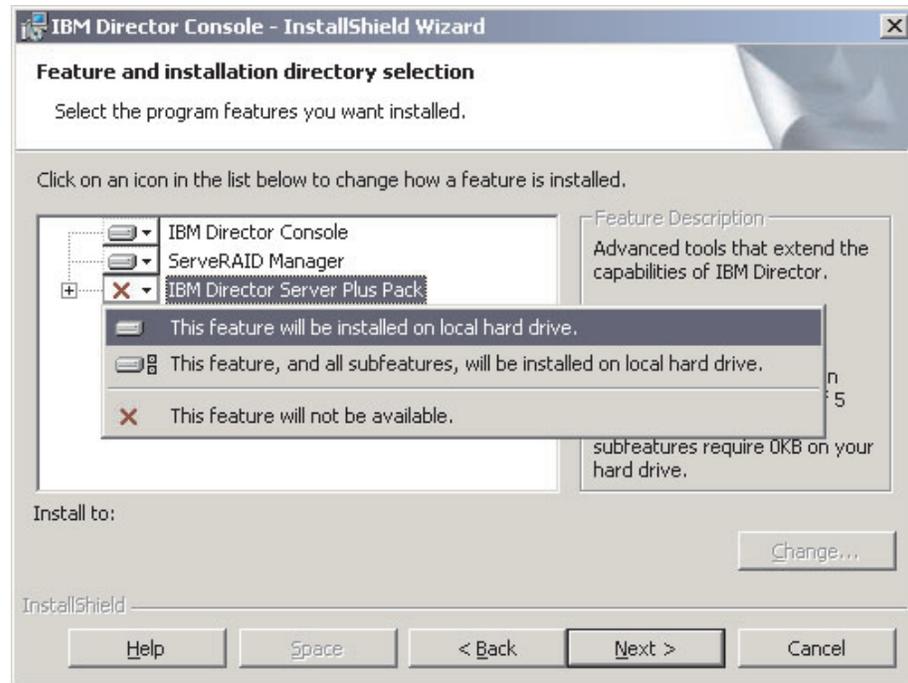


Figure 22. Installing IBM Director Console: Installing the Server Plus Pack

**Notes:**

- a. Until you install the Server Plus Pack extensions on the managed systems, you can run the Server Plus Pack tasks only against the management server.
  - b. Rack Manager will not function until the Rack Manager component, which is on the *IBM Director Server Plus Pack* CD, is installed on the management server.
11. Click **Next**. The “Ready to Install the Program” window opens.
  12. Click **Install**. The “Installing IBM Director Management Console” window opens. The status bar displays the progress of the installation. When the installation is completed, the “InstallShield Wizard Completed” window opens.
  13. Click **Finish**.
  14. Remove the *IBM Director 4.20* CD from the CD-ROM drive.

## Performing an unattended installation of IBM Director Console

You can perform an unattended installation of IBM Director Console using a response file, which provides answers to the questions that are posed by the InstallShield wizard. You can use this method to create a standard installation file that can be used on many systems.

Complete the following steps to install IBM Director Console:

1. Insert the *IBM Director 4.20* CD into the CD-ROM drive.
2. Copy the *dircon.rsp* file to a local directory. This file is in the *director\console\windows\i386* directory on the *IBM Director 4.20* CD.
3. From Windows Explorer, right-click the copy of the *dircon.rsp* file and then click **Properties**. The “*dircon.rsp* Properties” window opens. Clear the **Read-Only** check box and click **OK**.

4. Open the copy of the `dircon.rsp` file in an American Standard Code for Information Interchange (ASCII) text editor.
5. Modify and save the `dircon.rsp` file. This file follows the Windows initialization (INI) file format and is fully commented.
6. Change to the directory that contains the IBM Director Console installation file (`ibmsetup.exe`). This file is in the `director\console\windows\i386` directory on the *IBM Director 4.20 CD*.
7. From the command prompt, type the following command and press Enter:  
`ibmsetup.exe installationtype rsp="responsefile.rsp"`

where:

- *installationtype* is one of the following commands:
    - **unattended** shows the progress of the installation but does not require any user input.
    - **silent** suppresses all output to the screen during installation.
  - *responsefile.rsp* is the path and name of the response file that you created in step 5.
8. When the installation is completed, remove the *IBM Director 4.20 CD* from the CD-ROM drive.

---

## Chapter 6. Installing IBM Director Agent

This chapter contains instructions for installing IBM Director Agent 4.20. If you are upgrading IBM Director Agent, go to Chapter 12, “Upgrading IBM Director Agent,” on page 169.

### Notes:

1. Do not install the Management Processor Assistant (MPA) Agent on an @server blade server.
2. Do not install ServeRAID Manager on a system running VMware Console or a guest operating system.

---

### Preparing to install IBM Director Agent on an xSeries server

Before you install IBM Director Agent, make sure that you have installed all necessary device drivers. This might require installing service processor device drivers or the IBM LM78 and SMBus device drivers for Linux.

#### Service processor device drivers

If you plan to install IBM Director Agent on an xSeries server that contains one of the following service processors, make sure that the service processor device driver has been installed:

- Advanced System Management processor
- Advanced System Management PCI Adapter
- Remote Supervisor Adapter
- Remote Supervisor Adapter II

If the device driver is not installed before you install IBM Director Agent, the power indications provider might not be installed. This component monitors power supplies and generates alerts in the event of failure.

#### IBM LM78 and SMBus device drivers for Linux

If you plan to install IBM Director Agent on an xSeries server running Linux, you might have to install either or both the LM78 and SMBus device drivers for Linux. These device drivers ensure that certain IBM Director tasks and functions work properly.

The following table contains information about these device drivers, when they must be installed, and what they do.

*Table 18. Installing IBM Director Agent: IBM LM78 and SMBus device drivers for Linux*

Device driver	When it is needed	What it does
LM78	If either of the following conditions apply: <ul style="list-style-type: none"><li>• The server is an xSeries 225, machine type 8647 server.</li><li>• The server contains an integrated systems management processor (ISMP).</li></ul>	The LM78 device driver ensures that IBM Director Server receives memory and processor PFA alerts.
SMBus	If the server does not contain one of the following service processors: <ul style="list-style-type: none"><li>• IPMI baseboard management controller</li><li>• Remote Supervisor Adapter</li><li>• Remote Supervisor Adapter II</li></ul>	The SMBus device driver ensures that the Management Processor Assistant tasks and System Health Monitoring function properly.

## Downloading and installing the LM78 and SMBus device drivers

Perform the following steps to install either the IBM LM78 or SMBus device driver:

1. Download the TAR.GZ file that contains the source RPM file from the IBM Web site.
2. Build the binary RPM file.
3. Install the binary RPM file on the system on which you will install IBM Director Agent.

### Downloading the IBM LM78 and SMBus device drivers

The following table provides information about the TAR.GZ files that contain the source RPM files for the LM78 and SMBus device drivers.

Table 19. Installing IBM Director Agent: Source files for the LM78 and SMBus device drivers

Device driver	Operating system	File name
LM78	Red Hat Linux VMware ESX Server	dir4.20_lm78_redhatlinux.tar.gz
	SUSE LINUX	dir4.20_lm78_suselinux.tar.gz
SMBus	Red Hat Linux VMware ESX Server	dir4.20_smb_redhatlinux.tar.gz
	SUSE LINUX	dir4.20_smb_suselinux.tar.gz

You can download the files from the IBM Systems Management Software:

Download/Electronic Support page at

[http://www.ibm.com/pc/us/eserver/xseries/systems\\_management/dwnl.html](http://www.ibm.com/pc/us/eserver/xseries/systems_management/dwnl.html).

### Building the binary RPM file

You must build the binary RPM file on a system with the same kernel version and hardware configuration as the system on which you will install IBM Director Agent. Make sure that the hardware configuration is similar in regard to the number of processors.

Complete the following steps to build either the LM78 or SMBus device driver:

1. Configure a system with the applicable operating system and hardware configuration. Verify that the Linux kernel source is installed and properly configured.
2. Decompress the TAR.GZ file that contains the source RPM file.
3. To install the source RPM file, from a command prompt, type one of the following commands and press Enter:

<b>Red Hat Linux and VMware ESX Server</b>	<code>rpm -ivh driver-src-redhat-4.20-1.i386.rpm</code>
<b>SUSE LINUX</b>	<code>rpm -ivh driver-src-suse-4.20-1.i386.rpm</code>

where *driver* is either *ibmlm78* or *ibmsmb*. This creates a binary RPM file in either the `/usr/local/ibmsmb` or `/usr/local/ibmlm78` directory, depending on which source RPM file you installed.

## Installing the IBM LM78 or SMBus device driver

**Note:** In this procedure, *driver* is one of the following strings:

---

<b>For the IBM LM78 device driver</b>	ibmlm78
<b>For the IBM SMBus device driver</b>	ibmsmb

---

Complete the following steps to install either the IBM LM78 or SMBus device driver:

1. If you built the binary RPM file on another server, create a `/usr/local/ibm/driver` directory on the server where you will install IBM Director Agent. Copy the binary RPM file to that directory.
2. Change to the `/usr/local/driverb` directory.
3. To install the device driver, from a command prompt, type the following command and press Enter:

```
rpm -ivh driver-4.20-1.i386.rpm
```

Issuing the command accomplishes the following tasks:

- Uncompresses and untars the archive into the `/usr/local/driver` directory
- Copies the device driver, shared library, and all configuration files to their appropriate locations
- Loads the device driver

---

## Installing IBM Director Agent on AIX

**Note:** Make sure that the following filesets are installed before you install IBM Director Agent:

- bos.perf.perfstat
- bos.perf.libperfstat

Complete the following steps to install IBM Director Agent on AIX:

1. Insert the *IBM Director 4.20* CD into the CD-ROM drive.
2. To mount the CD-ROM drive, type the following command and press Enter:

```
mount -v cdrfs -o ro,nocase /dev/cd0 /mnt
```

where `dev/cd0` is the specific device file for the CD-ROM block device, and `mnt` is the mount point of the CD-ROM drive.

3. To change to the directory where IBM Director Agent is located, type the following command and press Enter:

```
cd /mnt/director/agent/aix
```

where `mnt` is the mount point of the CD-ROM drive.

4. To install IBM Director Agent, type the following command and press Enter:  

```
installp -acXYd. IBM.Director.Agent.IBMDirA
```
5. To enable encryption or change security settings, type the following command and press Enter:  

```
/opt/ibm/director/bin/cfgsecurity
```
6. To start IBM Director Agent, type the following command and press Enter:

```
/opt/ibm/director/bin/twgstart
```

7. To unmount the CD-ROM drive, type the following command and press Enter:  

```
umount /mnt
```

  
where *mnt* is the mount point of the CD-ROM drive.
8. Remove the *IBM Director 4.20* CD from the CD-ROM drive.

After IBM Director Agent is installed, you can enable the Wake on LAN feature. See “Enabling the Wake on LAN feature” on page 198.

---

## Installing IBM Director Agent on i5/OS

See the Virtualization Engine documentation for instructions for installing IBM Director Server on i5/OS. The Virtualization Engine documentation is part of the IBM @server Information Center at <http://www.ibm.com/servers/library/infocenter>.

After you have installed IBM Director Agent, complete the following steps to enable encryption:

1. To stop IBM Director Server, from a Qshell session, type the following command and press Enter:  

```
/qibm/userdata/director/bin/twgend
```
2. Using an ASCII text editor or the OS/400 Edit File (EDTF) command, open the `/QIBM/ProdData/Java400/jdk13/lib/security/java.security` file.
3. Uncomment the following line by removing the hash (#) at the beginning of the line:  

```
security.provider.3=com.ibm.crypto.provider.IBMJCE
```
4. To start IBM Director Agent, type the following command and press Enter:  

```
/qibm/userdata/director/bin/twgend
```

---

## Installing IBM Director Agent on Linux

### Notes:

1. Make sure that the operating-system password-encryption method is set to message digest 5 (MD5) or DES.
2. If you want to use the Remote Session task on the managed system, make sure that the package that contains telnetd is installed and configured. This is usually in the `telnet_server_version.i386.RPM` package, where *version* is the code level of your Linux distribution.
3. Before you install IBM Director Agent on either Red Hat Enterprise Linux AS, version 3.0 (32-bit) or Red Hat Enterprise Linux AS, version 3.0, for AMD64 (64-bit), make sure that the following RPM file is installed:  

```
compat-libstdc++-7.3-2.96.122.i386.rpm
```
4. The support for installing IBM Director Agent on operating systems for IBM iSeries and pSeries is only available only through the IBM Virtualization Engine and the *IBM Director 4.20* CD shipped with certain BladeCenter chassis.

Complete the following steps to install IBM Director Agent on Linux:

1. Insert the *IBM Director 4.20* CD into the CD-ROM drive.
2. If the CD does not automount, go to step 3 on page 67. If the CD automounts, type the following command and press Enter:  

```
umount /mnt/cdrom
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

3. Type the following command and press Enter:

```
mount -t iso9660 -o map=off /dev/cdrom /mnt/cdrom
```

where *dev/cdrom* is the specific device file for the CD-ROM block device and *mnt/cdrom* is mount point of the CD-ROM drive.

4. Change to the directory where the installation script is located. Type the following command and press Enter:

```
cd /mnt/cdrom/director/agent/linux/location/
```

where *mnt/cdrom* is the mount point of the CD-ROM drive, and *location* is one of the following strings:

---

<b>For 32-bit operating systems or operating systems for AMD64</b>	i386
<b>For operating systems for Intel Itanium</b>	ia64
<b>For operating systems for IBM iSeries and IBM pSeries</b>	ppc

---

5. If you want to customize the installation, go to step 6. If you want to accept the default settings for the installation, type the following command and press Enter:

```
./dirinstall
```

Go to step 10.

6. To customize the installation, copy the installation script to a local directory. Type the following command and press Enter:

```
cp dirinstall /directory/dirinstall
```

where *directory* is the local directory.

7. Open an ASCII text editor and modify the “User configuration” section of the *dirinstall* script. This file is fully commented.

You can specify the location of the RPM files, select the IBM Director Agent features that you want to install, and select log file options.

8. Save the modified installation script.
9. To install IBM Director, type the following command and press Enter:

```
/directory/dirinstall
```

where *directory* is the local directory to which you copied the installation script.

10. To enable encryption or change security settings, type the following command and press Enter:

```
/opt/Variable/director/bin/cfgsecurity
```

where *Variable* is one of the following strings:

---

<b>For 32-bit operating systems or operating systems for AMD64</b>	IBM
<b>For operating systems for IBM iSeries and IBM pSeries</b>	ibm

---

**Note:** Encryption is not supported on managed systems running either of the following operating systems:

- Red Hat Enterprise Linux AS, version 3.0, for Intel Itanium
- SUSE LINUX Enterprise Server 8 for Itanium Processor Family

11. To start IBM Director Agent, type the following command and press Enter:

```
/opt/Variable/director/bin/twgstart
```

where *Variable* is one of the following strings:

---

<b>For 32-bit operating systems or operating systems for AMD64</b>	IBM
--	-----

---

<b>For operating systems for Intel Itanium and IBM iSeries and IBM pSeries</b>	ibm
--	-----

---

12. To unmount the CD-ROM drive, complete the following steps:

- a. Type `cd /` and press Enter.
- b. Type the following command and press Enter:

```
umount /mnt/cdrom
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

13. Remove the *IBM Director 4.20* CD from the CD-ROM drive.

After IBM Director Agent is installed, you can enable the Wake on LAN feature. See “Enabling the Wake on LAN feature” on page 198.

To enable SNMP Access and Trap Forwarding, you must install and configure Net-SNMP, version 5.0.9. See “Enabling SNMP Access and Trap Forwarding for Linux” on page 198.

For information about installing the IBM Director Server Plus Pack extensions, see Chapter 9, “Installing IBM Director extensions,” on page 131

---

## Installing IBM Director Agent on NetWare

### Notes:

1. (xSeries servers only) Install the MPA Agent only if the server has one of the following service processors installed:
  - Advanced System Management processor
  - Advanced System Management PCI adapter
  - Remote Supervisor Adapter
  - Remote Supervisor Adapter II
2. To install IBM Director Agent, you must log on to the NetWare server from a Windows workstation running the NetWare Client for Windows. The SYS volume must be mapped as a drive to the system running Windows. Also, you must have administrator or supervisor access on the NetWare server.

Complete the following steps to install IBM Director Agent on NetWare:

1. Insert the *IBM Director 4.20* CD into the CD-ROM drive of the system running Windows. If the autorun window opens, close it.
2. Start Windows Explorer and open the `\director\agent\netware` directory.
3. Double-click **setup.exe**. The InstallShield wizard starts.
4. Click **Next**. The “Installing IBM Director Agent” window opens.

5. Click **Next** to accept the license agreement. The “Choose destination location” window opens.

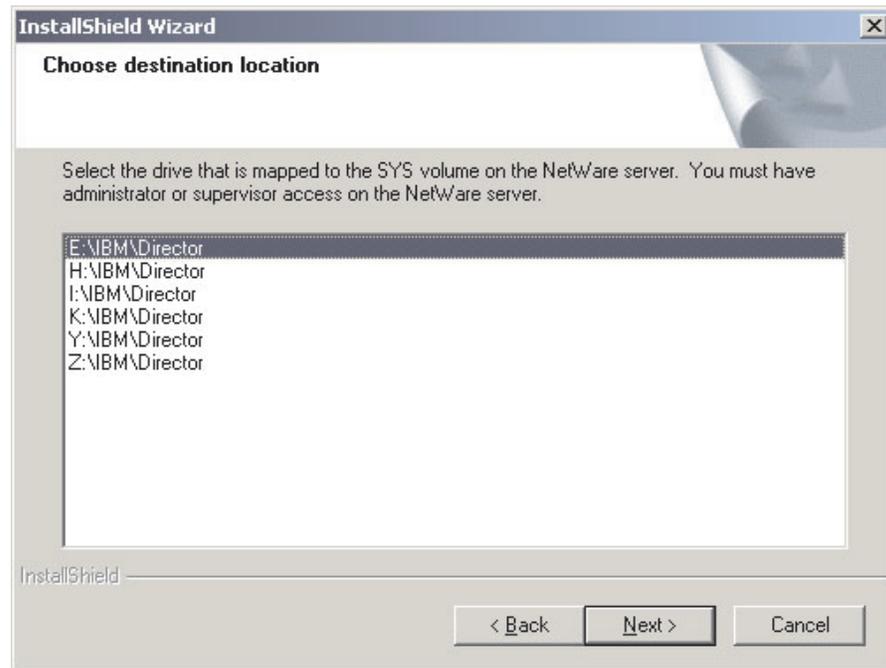


Figure 23. Installing IBM Director Agent on NetWare: “Choose destination location” window

6. Click the drive that is mapped to the SYS volume on the server running NetWare; then, click **Next**. The “Select Components” window opens.

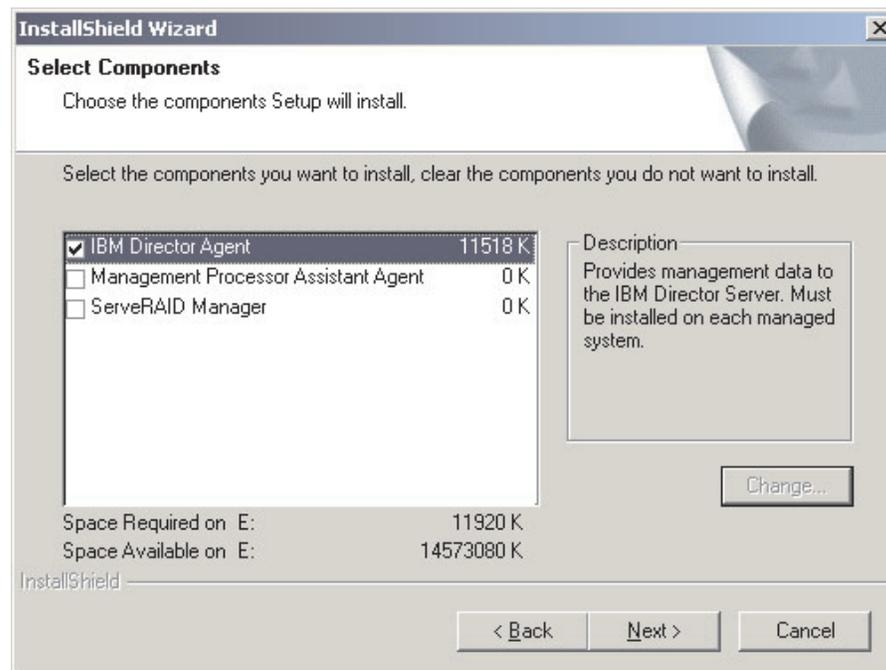


Figure 24. Installing IBM Director Agent on NetWare: “Select Components” window

IBM Director Agent is selected automatically for installation.

7. Select the check boxes for the IBM Director Agent features that you want to install:

**Management Processor Assistant Agent**

Enables communication with service processors in IBM xSeries and Netfinity servers

**ServeRAID Manager**

Manages and monitors IBM ServeRAID adapters and integrated SCSI controllers with RAID capabilities

8. Click **Next**. The “Setup Status window” opens, and IBM Director Agent installation begins. When the installation is completed, the “InstallShield Wizard complete” window opens.

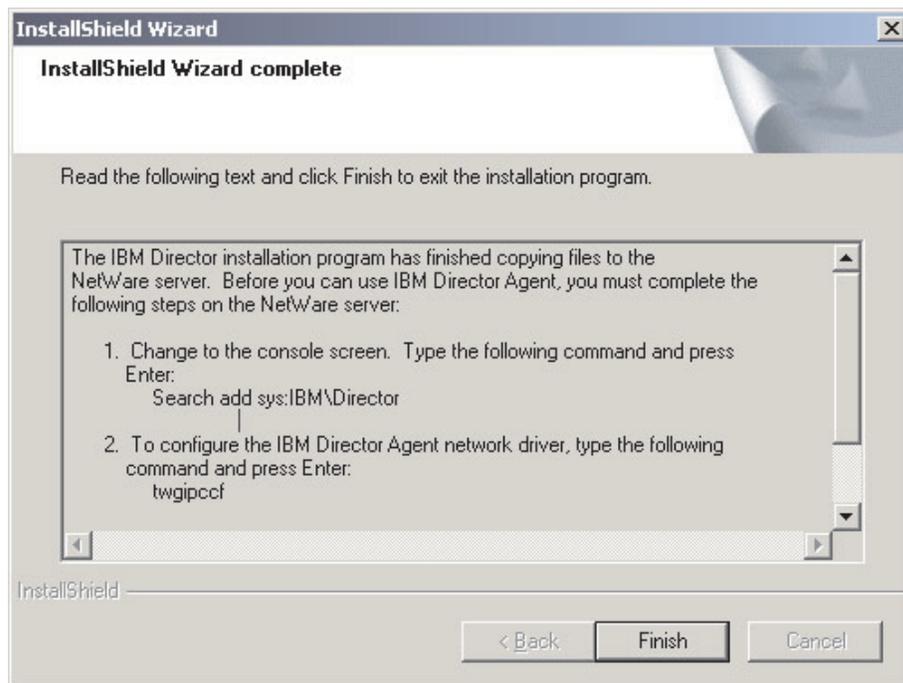


Figure 25. Installing IBM Director Agent on NetWare: “InstallShield Wizard complete” window

9. Click **Finish**.
10. Remove the *IBM Director 4.20* CD from the CD-ROM drive.
11. On the server running NetWare, change to the console screen.
12. From the console, type the following command and press Enter:  
Search add sys:IBM\Director
13. To define the protocols to use for communication between IBM Director Server and IBM Director Agent, type the following command and press Enter:  
twgipccf

**Note:** If you disable TCPIP (all adapters) and enable an individual device driver on a system with multiple network adapters, IBM Director Agent will receive *only* those data packets that are addressed to the individual adapter.

14. To start IBM Director Agent, type the following command and press Enter:

```
load twgipc
```

IBM Director Agent will start automatically whenever the server running NetWare starts.

For information about installing the IBM Director Server Plus Pack extensions, see Chapter 9, “Installing IBM Director extensions,” on page 131.

---

## Installing IBM Director Agent on Windows (32-bit)

This section provides information about installation prerequisites and instructions for installing IBM Director Agent using the InstallShield wizard. The wizard can be used in a standard interactive mode, or you can perform an unattended installation using a response file to provide answers to the questions that the wizard poses.

Before you install IBM Director Agent, make sure that you have uninstalled any incompatible files and installed any necessary prerequisites and device drivers.

Consider the following information:

1. Early versions of Active PCI Manager are not compatible with IBM Director. Make sure that you have uninstalled any Active PCI Manager, versions 1.0, 1.1, and 3.1.1, components.
2. (Windows NT 4.0 only) Make sure that you have installed the following prerequisites:
  - Microsoft Run-Time Components for Visual C++ Applications: You can download `vcredist.exe`, a self-extracting, executable file from <http://www.microsoft.com>. For more information, see Microsoft Knowledge Base Article 259403.
  - Windows Management Instrumentation (WMI) CORE 1.5: You can download `wmint4.exe`, a self-extracting, executable file from <http://www.microsoft.com>.

## Installing IBM Director Agent using the InstallShield wizard

Complete the following steps to install IBM Director Agent on Windows:

1. Insert the *IBM Director 4.20* CD into the CD-ROM drive.
2. If the installation program starts automatically and the InstallShield wizard starts, go to step 4. Otherwise, click **Start** → **Run**.
3. In the **Open** field, type the following command and press Enter:

```
e:\setup.exe
```

where *e* is the drive letter of the CD-ROM drive. The installation program starts, and the “IBM Director” window opens.

4. Click **Install IBM Director**. The “IBM Director Installation” window opens.
5. Click **IBM Director Agent installation**. The “IBM Director Agent Installation” window opens.
6. Click **32-bit installation**. The InstallShield wizard starts, and the “Welcome to the InstallShield Wizard” window opens.
7. Click **Next**. The “License Agreement” window opens.
8. Click **I accept the terms in the license agreement** and click **Next**. The “Feature and installation directory selection” window opens.

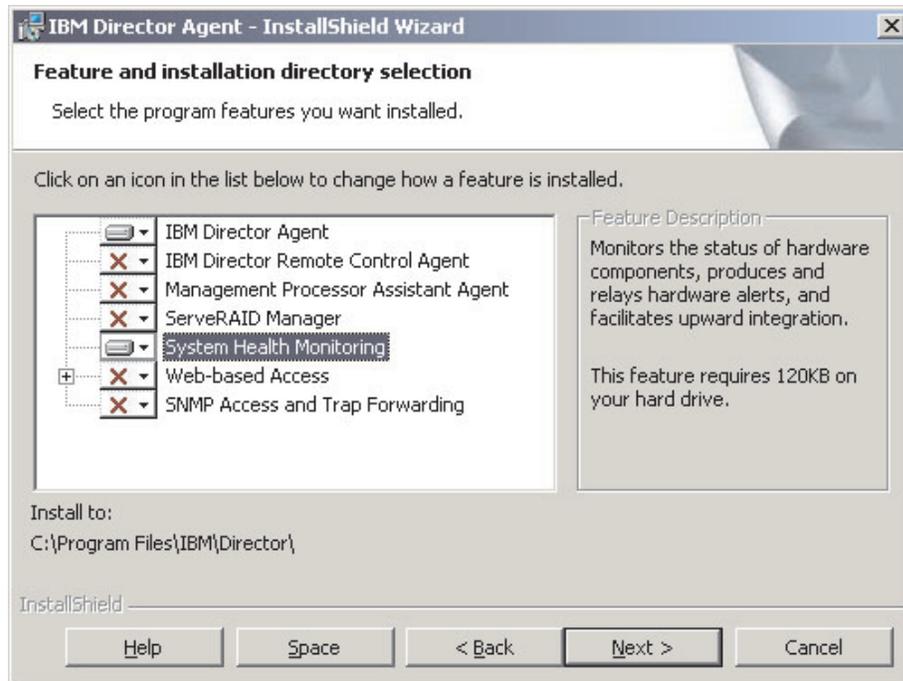


Figure 26. Installing IBM Director Agent on Windows: “Feature and installation directory selection” window

IBM Director Agent and System Health Monitoring are selected automatically for installation; a hard disk drive icon  is displayed to the left of the components.  is displayed to the left of the optional features that are not selected by default.

9. Select the IBM Director Agent features that you want to install:

**IBM Director Remote Control Agent**

Enables a system administrator to perform remote desktop functions on the managed system

**Management Processor Assistant Agent**

Enables communication with service processors in IBM xSeries and Netfinity servers

**ServeRAID Manager**

Manages and monitors IBM ServeRAID adapters and integrated SCSI controllers with RAID capabilities

**System Health Monitoring**

Monitors the status of hardware components, produces and relays hardware alerts, and facilitates upward integration

**Web-based Access**

Enables system administrators to access managed-system data through a Web browser or the Microsoft Management Console (MMC)

**SNMP Access and Trap Forwarding**

Enables access to managed-system data and alerts through SNMP

To select a feature, click  to the left of the feature name. A menu opens.

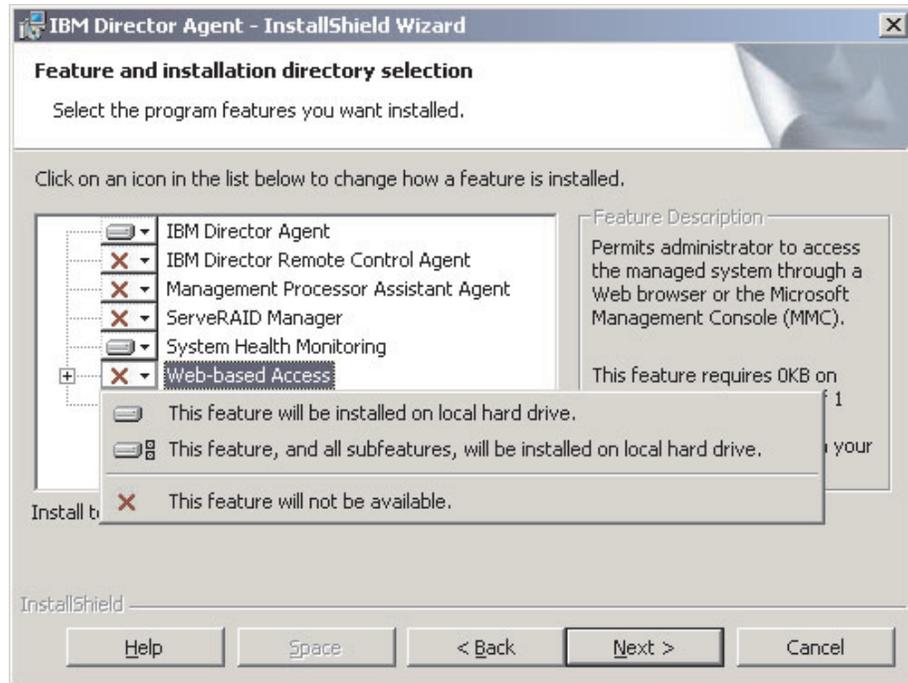


Figure 27. Installing IBM Director Agent on Windows: “Feature and installation directory selection” window

To install the feature, click either **This feature will be installed on local hard drive** or **This feature, and all subfeatures, will be installed on local hard drive**.

10. Click **Next**. The “Security settings” window opens.

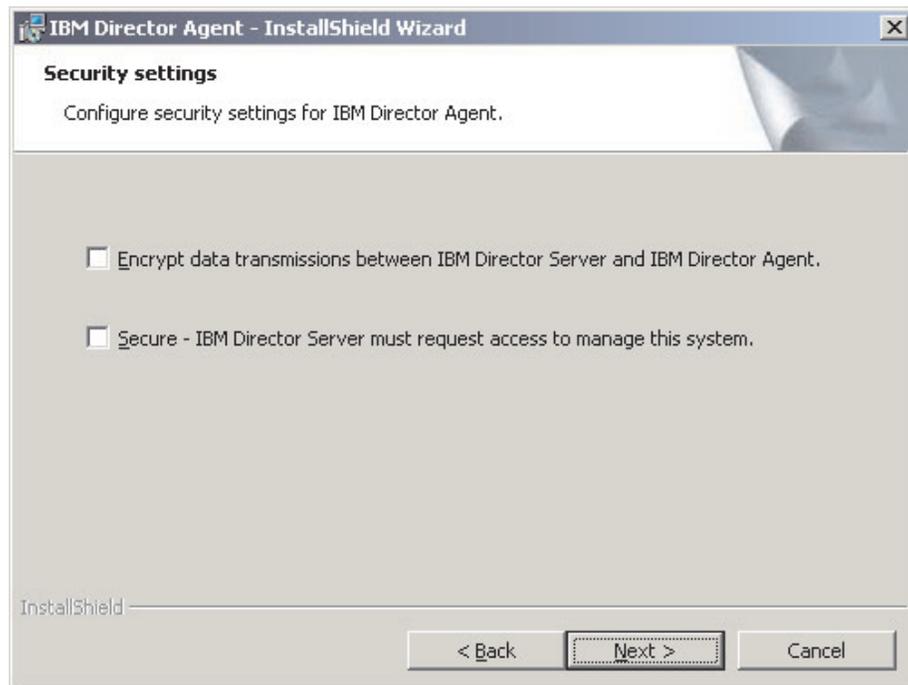


Figure 28. Installing IBM Director Agent on Windows: “Security settings” window

11. If you do not want to encrypt transmissions between IBM Director Server and IBM Director Agent, go to step 12. Otherwise, select the **Encrypt data transmissions between IBM Director Server and IBM Director Agent** check box.

**Note:** If encryption is enabled, the following conditions apply:

- The managed system is automatically secured, and the **Secure – IBM Director Server must request access to manage this system** check box is unavailable.
  - Only management servers with encryption enabled are able to communicate with the managed system.
12. To set IBM Director Agent to the secured state, select the **Secure – IBM Director Server must request access to manage this system** check box. This ensures that IBM Director Server cannot manage this system until it is granted access.
  13. Click **Next**. The “Software Distribution settings” window opens.

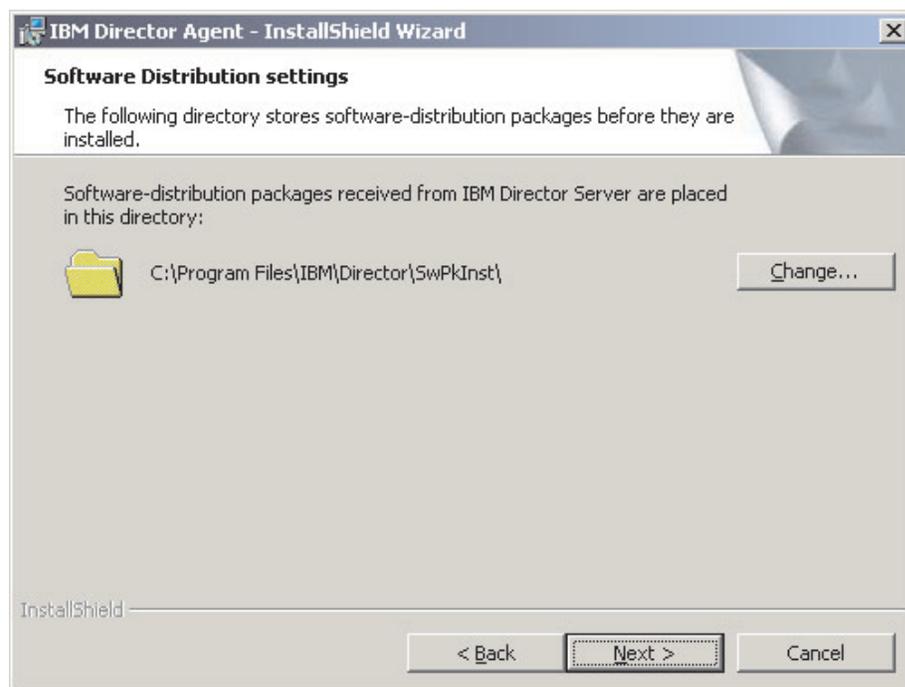


Figure 29. Installing IBM Director Agent on Windows: “Software Distribution settings” window

To select an alternative location for where software-distribution packages are stored before being applied to IBM Director Agent, click **Change** and select another directory.

14. Click **Next**. If you did not select to install the Web-based Access feature, go to step 16 on page 75. Otherwise, the “Web-based Access information” window opens.

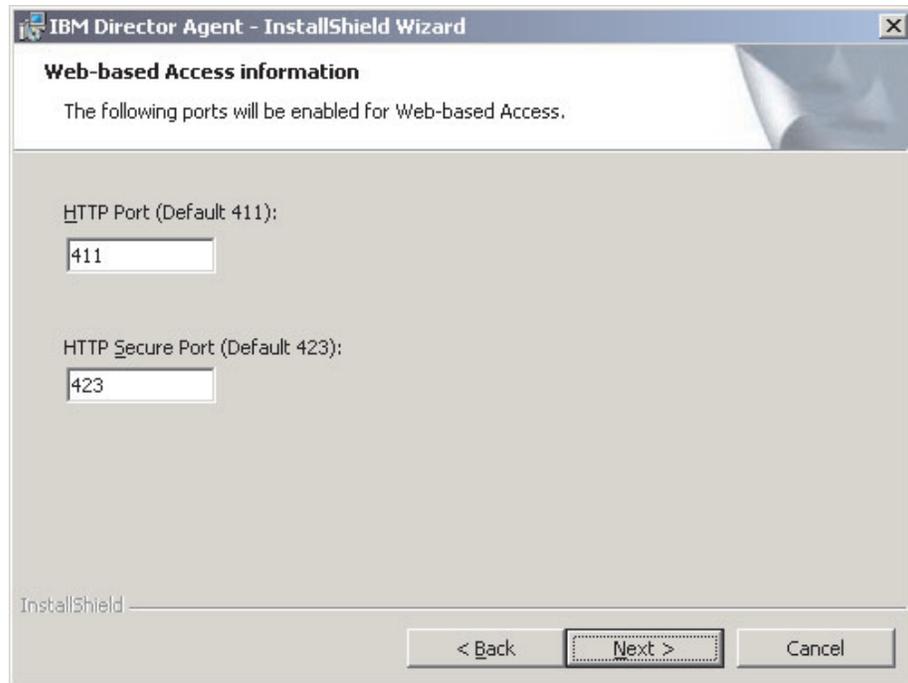


Figure 30. Installing IBM Director Agent on Windows: “Web-based Access information” window

15. Change the default HTTP port numbers (if necessary), and click **Next**. The “Ready to Install the Program” window opens.
16. Click **Install**. The “Installing IBM Director Agent” window opens. The status bar indicates the progress of the installation. When the installation is completed, the “Network driver configuration” window opens.

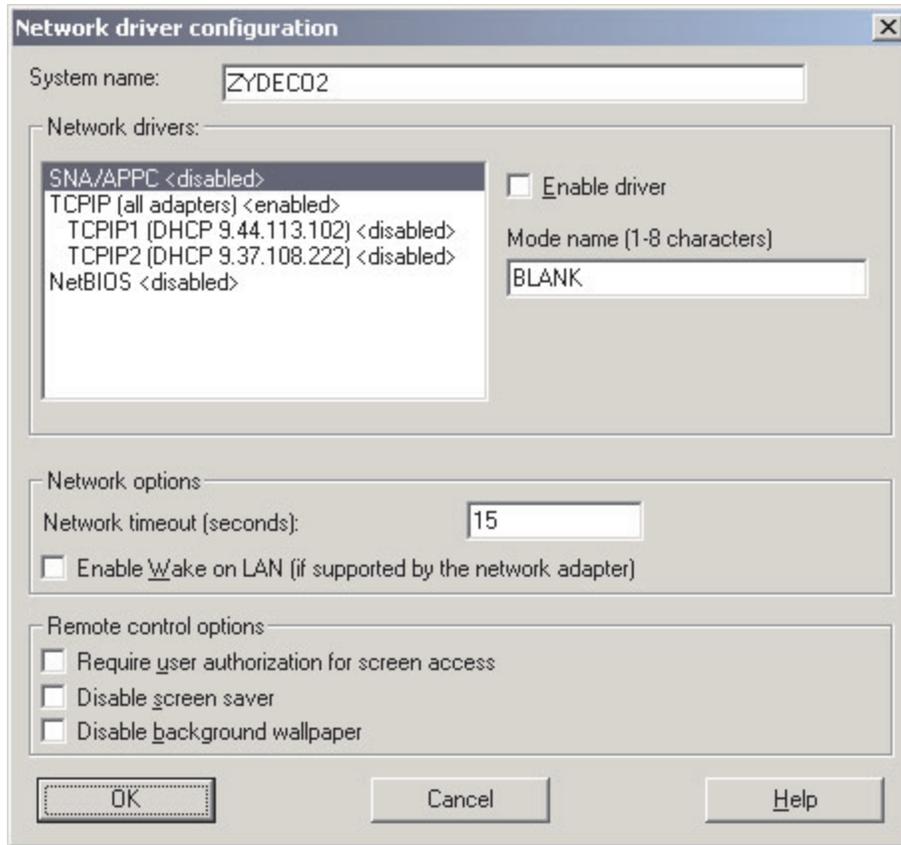


Figure 31. Installing IBM Director Agent on Windows: “Network driver configuration” window

17. In the **System Name** field, type the name that you want to be displayed in IBM Director Console. By default, this is the NetBIOS name of the managed system.
18. Define the communications protocols to use for communication between IBM Director Server and IBM Director Agent.
  - a. In the **Network drivers** field, TCPIP (all adapters) is enabled by default. To enable another protocol, select the protocol and then select the **Enable driver** check box.
 

**Note:** If you disable TCPIP (all adapters) and enable an individual device driver on a system with multiple network adapters, IBM Director Agent will receive *only* those data packets that are addressed to the individual adapter.
  - b. In the **Network timeout** field, type the number of seconds that IBM Director Server waits for a response from IBM Director Agent. By default, this is set to 15 seconds.
  - c. Click **Enable Wake on LAN** if the network adapter supports the Wake on LAN feature.
 

**Note:** To determine whether your server supports the Wake on LAN feature, see your server documentation.

19. If you selected to install the IBM Director Remote Control Agent, the following options are available:

**Require User Authorization for System Access**

Select this check box to request authorization from the local user before accessing the managed system remotely.

**Disable Screen Saver**

Select this check box to disable the screen saver when the managed system is controlled remotely.

**Disable Background Wallpaper**

Select this check box to disable desktop wallpaper when the managed system is controlled remotely. You might want to disable the wallpaper because complicated backgrounds slow down remote control and increase network traffic.

20. Click **OK**. The status bar displays the progress of the installation. When the installation is completed, the “InstallShield Wizard Completed” window opens.
21. Click **Finish**. The “IBM Director Agent Installer Information” window opens.
22. Remove the *IBM Director 4.20* CD from the CD-ROM drive.
23. Click **Yes** to restart your system.

For information about installing the IBM Director Server Plus Pack extensions, see Chapter 9, “Installing IBM Director extensions,” on page 131.

## Performing an unattended installation of IBM Director Agent

You can perform an unattended installation of IBM Director Agent using a response file, which provides answers to the questions posed by the InstallShield wizard. You can use this method to create a standard installation file that can be used on many systems.

Complete the following steps to install IBM Director Agent on Windows:

1. Insert the *IBM Director 4.20* CD into the CD-ROM drive.
2. Copy the `diragent.rsp` file to a local directory. This file is located in the `director\agent\windows\i386` directory on the *IBM Director 4.20* CD.
3. From Windows Explorer, right-click the copy of the `diragent.rsp` file and then click **Properties**. The “`diragent.rsp` Properties” window opens. Clear the **Read-Only** check box and click **OK**.
4. Open the copy of the `diragent.rsp` file in an ASCII text editor.
5. Modify and save the `diragent.rsp` file. This file follows the Windows INI file format and is fully commented.
6. Change to the directory that contains the IBM Director Agent installation file (`ibmsetup.exe`). This file is located in the `director\agent\windows\i386` directory on the *IBM Director 4.20* CD.

7. From the command prompt, type the following command and press Enter:  
`ibmsetup.exe installationtype rsp="responsefile.rsp" waitforme`

where:

- *installationtype* is one of the following commands:
    - **unattended** shows the progress of the installation but does not require any user input.
    - **silent** suppresses all output to the screen during installation.
  - *responsefile.rsp* is the path and name of the response file that you created in step 5 on page 77.
  - *waitforme* is an optional parameter that ensures that `ibmsetup.exe` process will not end until the installation of IBM Director Agent is completed.
8. If you issued the **unattended** command in step 7, restart the operating system when prompted to do so.
  9. Remove the *IBM Director 4.20* CD from the CD-ROM drive.

For information about installing the IBM Director Server Plus Pack extensions, see Chapter 9, “Installing IBM Director extensions,” on page 131.

---

## Installing IBM Director Agent on Windows (64-bit)

This section provides instructions for installing IBM Director Agent using the InstallShield wizard. The wizard can be used in a standard interactive mode, or you can perform an unattended installation using a response file to provide answers to the questions that the wizard poses.

### Installing IBM Director Agent using the InstallShield wizard

Complete the following steps to install IBM Director Agent on Windows:

1. Insert the *IBM Director 4.20* CD into the CD-ROM drive.
2. If the installation program starts automatically and the InstallShield wizard starts, go to step 4. Otherwise, click **Start** → **Run**.
3. In the **Open** field, type the following command and press Enter:

```
e:\setup.exe
```

where *e* is the drive letter of the CD-ROM drive. The installation program starts, and the “IBM Director” window opens.

4. Click **Install IBM Director**. The “IBM Director Installation” window opens.
5. Click **IBM Director Agent installation**. The “IBM Director Agent Installation” window opens.
6. Click **64-bit installation**. The InstallShield wizard starts, and the “Welcome to the InstallShield Wizard” window opens.
7. Click **Next**. The “License Agreement” window opens.
8. Click **I accept the terms in the license agreement** and click **Next**. The “Feature and installation directory selection” window opens.

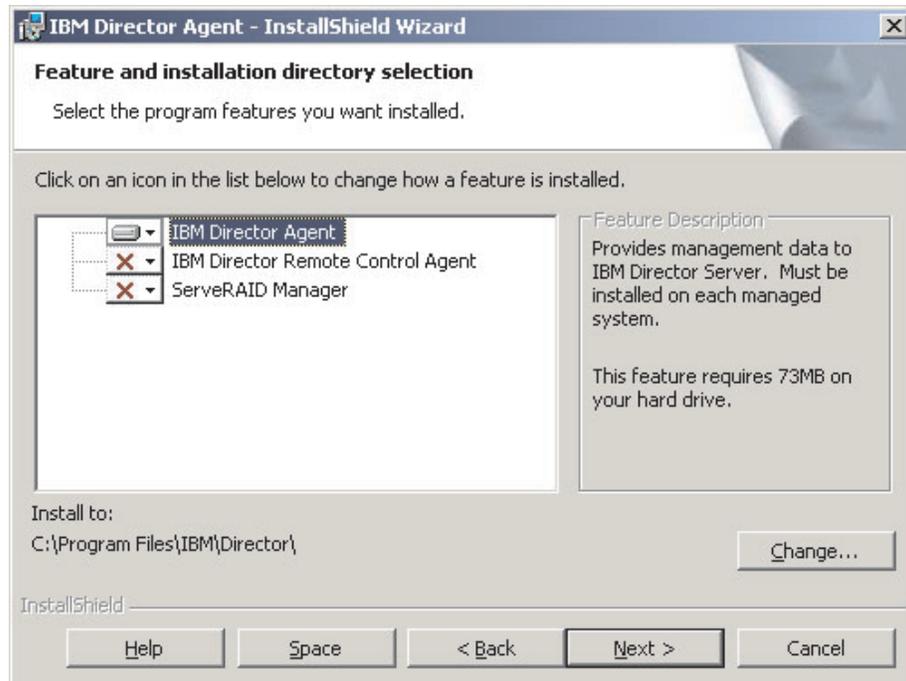


Figure 32. Installing IBM Director Agent on Windows: “Feature and installation directory selection” window

IBM Director Agent is selected automatically for installation; a hard disk drive icon  is displayed to the left of the component.  is displayed to the left of the optional features that are not selected by default.

9. Select the IBM Director Agent features that you want to install:

#### **IBM Director Remote Control Agent**

Enables a system administrator to perform remote desktop functions on the managed system.

#### **ServeRAID Manager**

Manages and monitors IBM ServeRAID adapters and integrated SCSI controllers with RAID capabilities.

To select a feature, click  to the left of the feature name. A menu opens. To install the feature, click **This feature will be installed on local hard drive** or **This feature, and all subfeatures, will be installed on local hard drive**.

10. Click **Next**. The “Security settings” window opens.

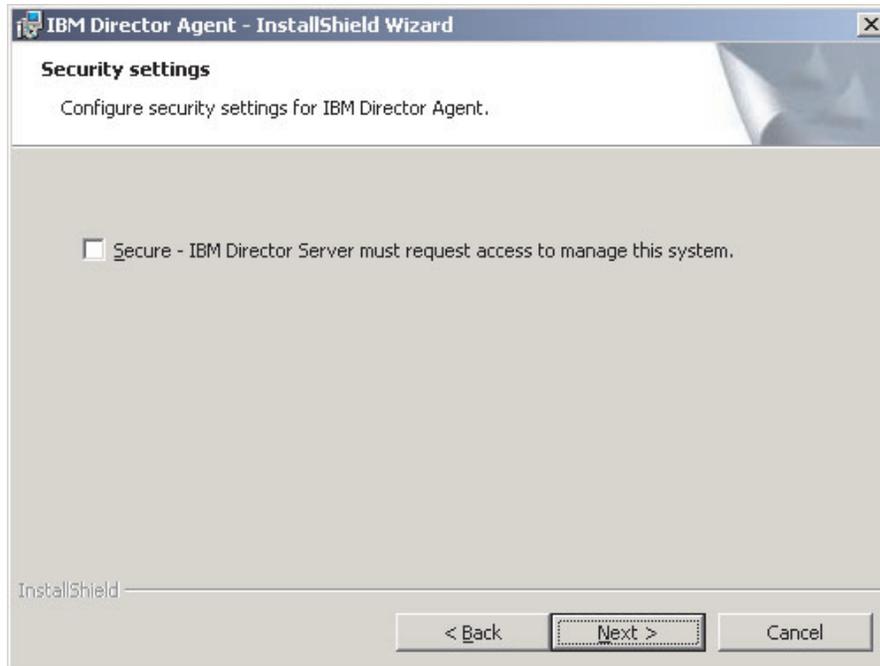


Figure 33. Installing IBM Director Agent on Windows: “Security settings” window

11. To set IBM Director Agent to the secured state, select the **Secure – IBM Director Server must request access to manage this system** check box. This ensures that IBM Director Server cannot manage this system until it is granted access.
12. Click **Next**. The “Software Distribution settings” window opens.

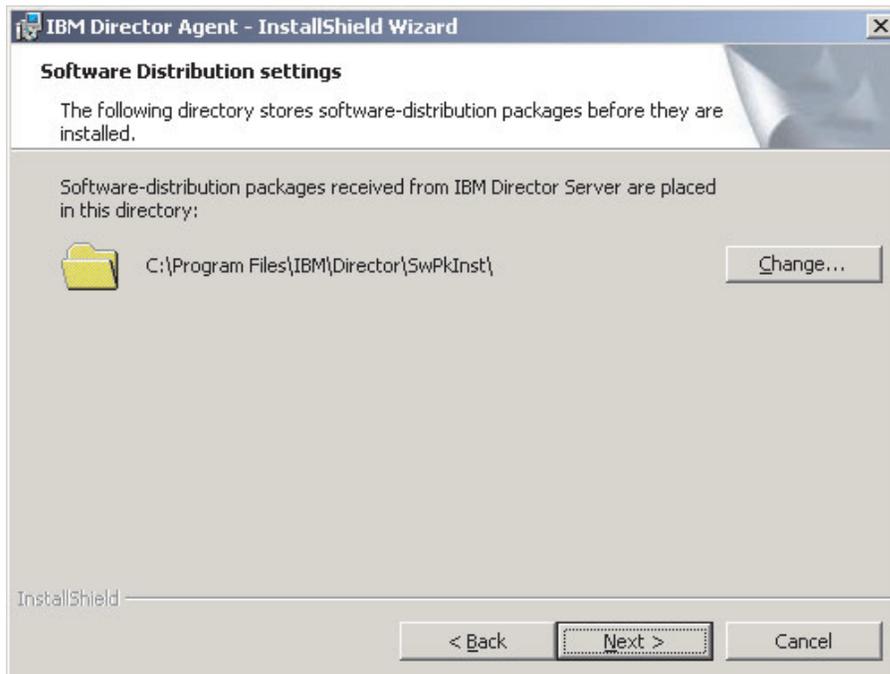


Figure 34. Installing IBM Director Agent on Windows: “Software Distribution settings” window

13. To select an alternative location for where software-distribution packages are stored before being applied to IBM Director Agent, click **Change** and select another directory.
14. Click **Next**. The “Ready to Install the Program” window opens.
15. Click **Install**. The “Installing IBM Director Agent” window opens.  
The status bar indicates the progress of the installation. When the installation is completed, the “Network driver configuration” window opens.

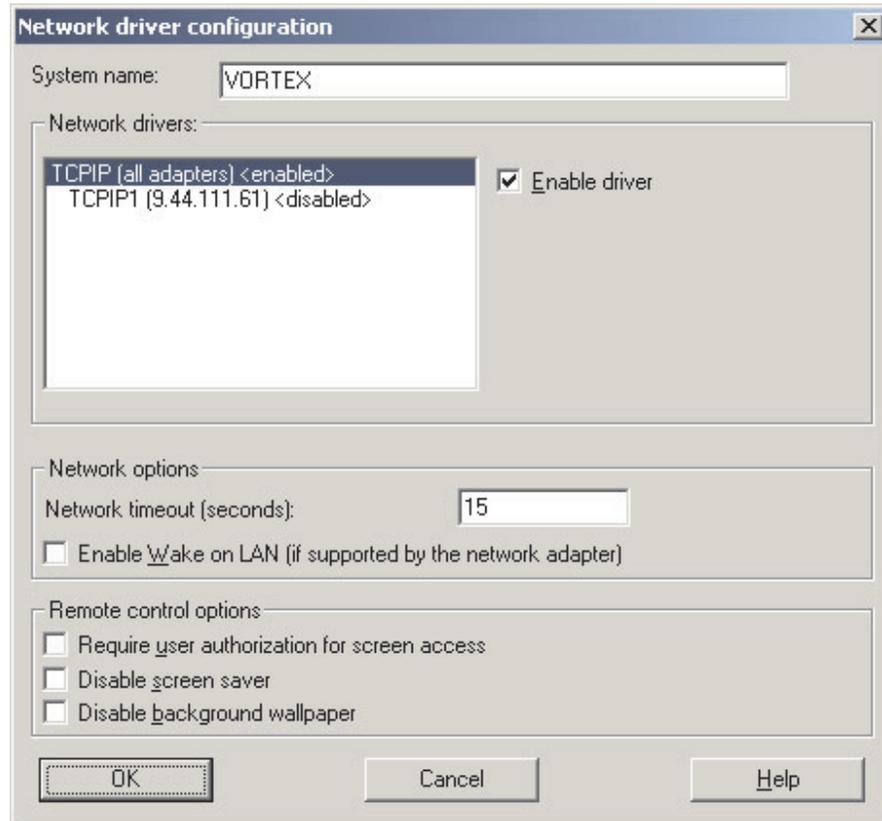


Figure 35. Installing IBM Director Agent on Windows: “Network driver configuration” window

16. In the **System Name** field, type the name that you want to be displayed in IBM Director Console. By default, this is the NetBIOS name of the managed system.
17. Define the communications protocols to use for communication between IBM Director Server and IBM Director Agent.
  - a. In the **Network drivers** field, TCPIP (all adapters) is enabled by default. To enable another protocol, select the protocol and then select the **Enable driver** check box.  
  
**Note:** If you disable TCPIP (all adapters) and enable an individual device driver on a system with multiple network adapters, IBM Director Agent will receive *only* those data packets that are addressed to the individual adapter.
  - b. In the **Network timeout** field, type the number of seconds that IBM Director Server waits for a response from IBM Director Agent. By default, this is set to 15 seconds.

- c. Click **Enable Wake on LAN** if the network adapter supports the Wake on LAN feature.

**Note:** To determine whether your server supports the Wake on LAN feature, see your server documentation.

18. If you selected to install the IBM Director Remote Control Agent, the following options are available:

**Require User Authorization for System Access**

Select this check box to request authorization from the local user before accessing the managed system remotely.

**Disable Screen Saver**

Select this check box to disable the screen saver when the managed system is controlled remotely.

**Disable Background Wallpaper**

Select this check box to disable desktop wallpaper when the managed system is controlled remotely. You might want to disable the wallpaper because complicated backgrounds slow down remote control and increase network traffic.

19. Click **OK**. The status bar displays the progress of the installation. When the installation is completed, the “InstallShield Wizard Completed” window opens.
20. Click **Finish**. The “IBM Director Agent Installer Information” window opens.
21. Remove the *IBM Director 4.20* CD from the CD-ROM drive.
22. Click **Yes** to restart your system.

## Performing an unattended installation of IBM Director Agent

You can perform an unattended installation of IBM Director Agent using a response file, which provides answers to the questions that are posed by the InstallShield wizard. You can use this method to create a standard installation file that can be used on many systems.

Complete the following steps to install IBM Director Agent on Windows:

1. Insert the *IBM Director 4.20* CD into the CD-ROM drive.
2. Copy the `diragent.rsp` file to a local directory. This file is in the `director\agent\windows\ia64` directory on the *IBM Director 4.20* CD.
3. From Windows Explorer, right-click the copy of the `diragent.rsp` file and then click **Properties**. The “`diragent.rsp` Properties” window opens. Clear the **Read-Only** check box and click **OK**.
4. Open the copy of the `diragent.rsp` file in an ASCII text editor.
5. Modify and save the `diragent.rsp` file. This file follows the Windows INI file format and is fully commented.
6. Change to the directory that contains the IBM Director Agent installation file (`ibmsetup.exe`). This file is in the `director\agent\windows\ia64` directory on the *IBM Director 4.20* CD.

7. From the command prompt, type the following command and press Enter:  
`ibmsetup.exe installationtype rsp="responsefile.rsp" waitforme`

where:

- *installationtype* is one of the following commands:
    - **unattended** shows the progress of the installation but does not require any user input.
    - **silent** suppresses all output to the screen during installation.
  - *responsefile.rsp* is the path and name of the response file that you created in step 5 on page 77.
  - *waitforme* is an optional parameter that ensures that `ibmsetup.exe` process will not end until the installation of IBM Director Agent is completed.
8. If you issued the **unattended** command in step 7 on page 78, restart the operating system when prompted to do so.
  9. Remove the *IBM Director 4.20* CD from the CD-ROM drive.



---

## Part 3. Configuring IBM Director



---

## Chapter 7. Configuring IBM Director

This chapter contains information about starting IBM Director Console, using the Event Action Plan wizard, setting discovery preferences and creating management processor objects, authorizing IBM Director users, configuring security settings, and setting up software distribution.

---

### Starting IBM Director Console

Complete the following steps to start IBM Director Console:

1. To start IBM Director Console, take one of the following actions:

---

<b>For Linux</b>	From a command prompt, type the following command and press Enter: twgcon
<b>For Windows</b>	Click <b>Start</b> → <b>Programs</b> → <b>IBM Director Console</b> .

---

The “IBM Director Login” window opens.



Figure 36. “IBM Director Login” window

2. In the **IBM Director Server** field, type the name of the management server.
3. In the **User ID** field, type one of the following strings:

---

<b>For Linux</b>	<i>UserID</i>
<b>For Windows</b>	<i>ComputerName\UserID</i>

---

where:

- *UserID* is a valid IBM Director user ID.
  - *ComputerName* is either the local computer name or the domain, depending on whether the IBM Director service account has domain or local privileges
4. In the **Password** field, type the password that corresponds to the user ID.
  5. Click **OK**. IBM Director Console starts.

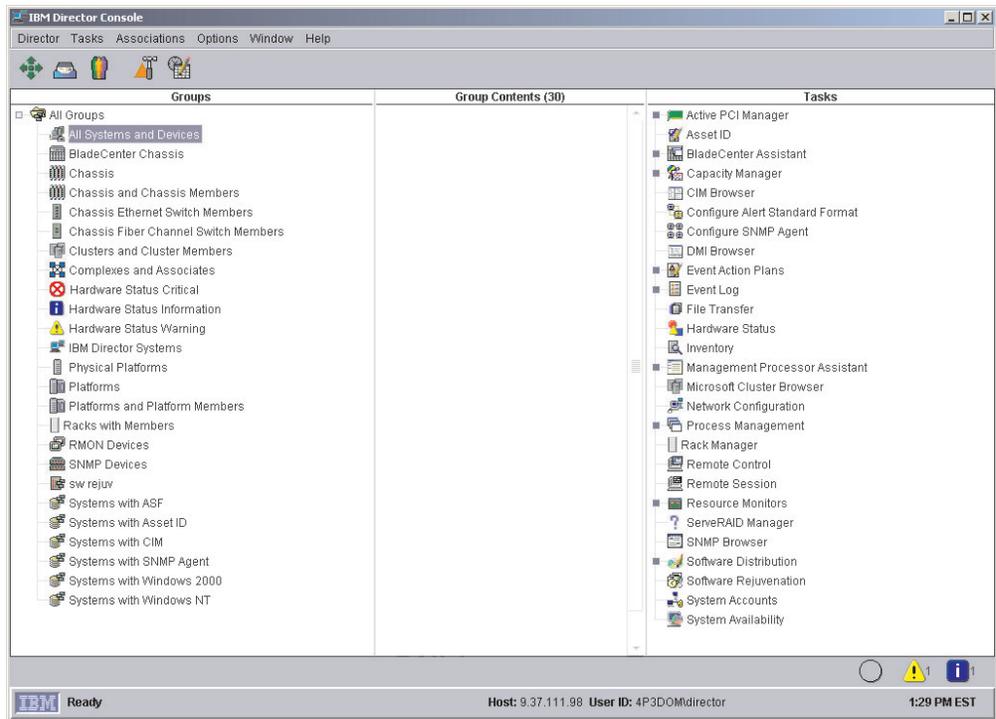


Figure 37. IBM Director Console

## Using the Event Action Plan wizard

The Event Action Plan wizard starts every time you log in to IBM Director Console, until you take one of the following actions:

- Use the Event Action Plan wizard to create an event action plan. You must go through the wizard and click **Finish** on the last window.
- Select the **Do not show this wizard again** check box and then close the Event Action Plan wizard.

If you take one of these actions, you are no longer able to access the Event Action Plan wizard. However, you can create or modify an event action plan using the Event Action Plan Builder. For more information, see the *IBM Director 4.20 Systems Management Guide*.

**Note:** You also can restrict access to the Event Action Plan wizard by removing users' access to the Event Action Plan Builder task. See "Creating user-account defaults" on page 97.

Complete the following steps to use the Event Action Plan wizard:

1. Start IBM Director Console. The Event Action Plan wizard starts, and the "Welcome to the Event Action Plan wizard" window opens.

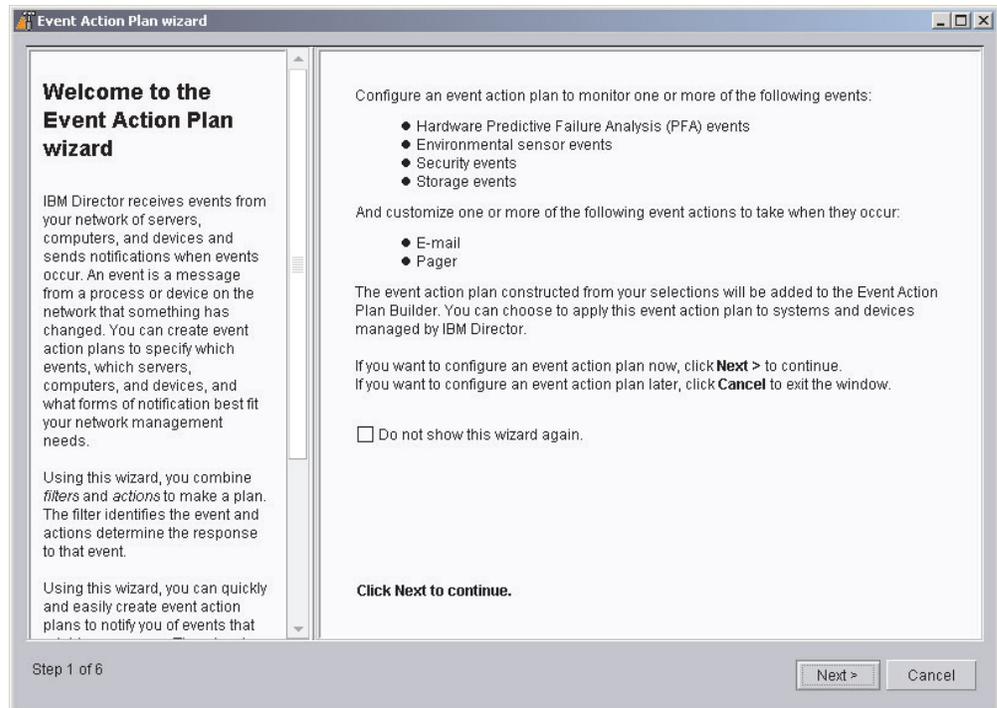


Figure 38. Event Action Plan wizard: “Welcome to the Event Action Plan wizard” window

2. Click **Next**. The “Select the event filters” window opens.

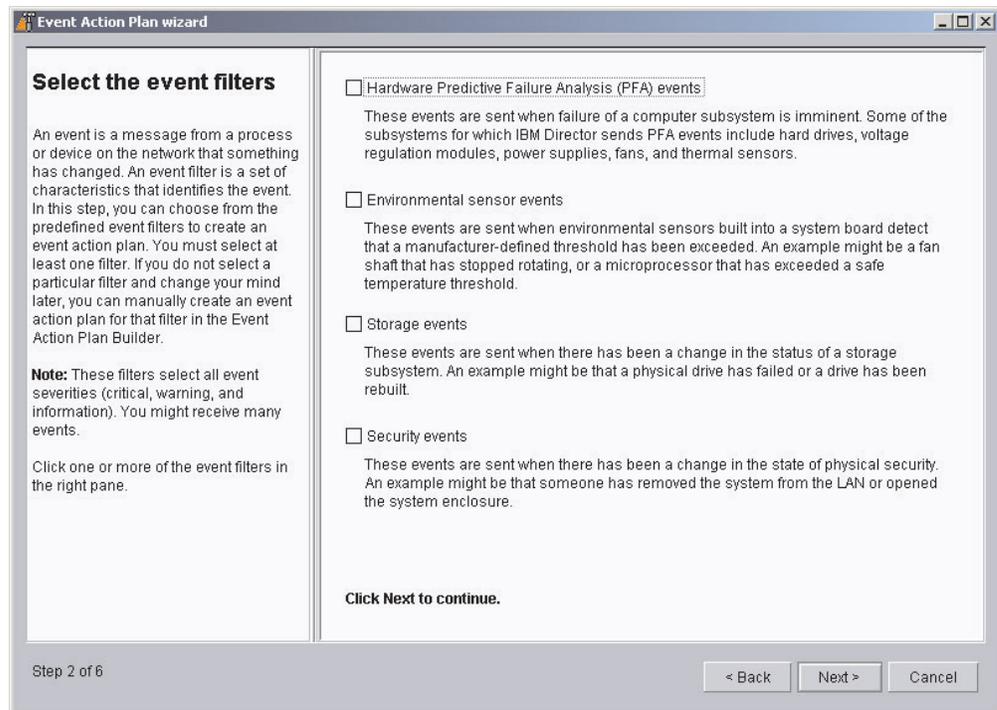


Figure 39. Event Action Plan wizard: “Select the event filters” window

3. Select the check boxes adjacent to the types of events you want to monitor. You can select the following event filters:

#### Hardware Predictive Failure Analysis (PFA) events

These events are sent when failure of a computer subsystem is imminent. Some of the subsystems for which IBM Director sends PFA events include hard disk drives, voltage regulation modules, power supplies, and thermal sensors.

#### Environmental sensor events

These events are sent when environmental sensors built into a system board detect that a manufacturer-defined threshold has been exceeded. An example might be a microprocessor that has exceeded a safe temperature threshold.

#### Storage events

These events are sent when there has been a change in the status of a storage subsystem. An example might be that a physical drive has failed or a logical drive has been rebuilt.

#### Security events

These events are sent when there has been a change in the status of physical security. An example might be that someone has removed the system from the LAN or opened the system enclosure.

4. Click **Next**. The “Select the notification” window opens.

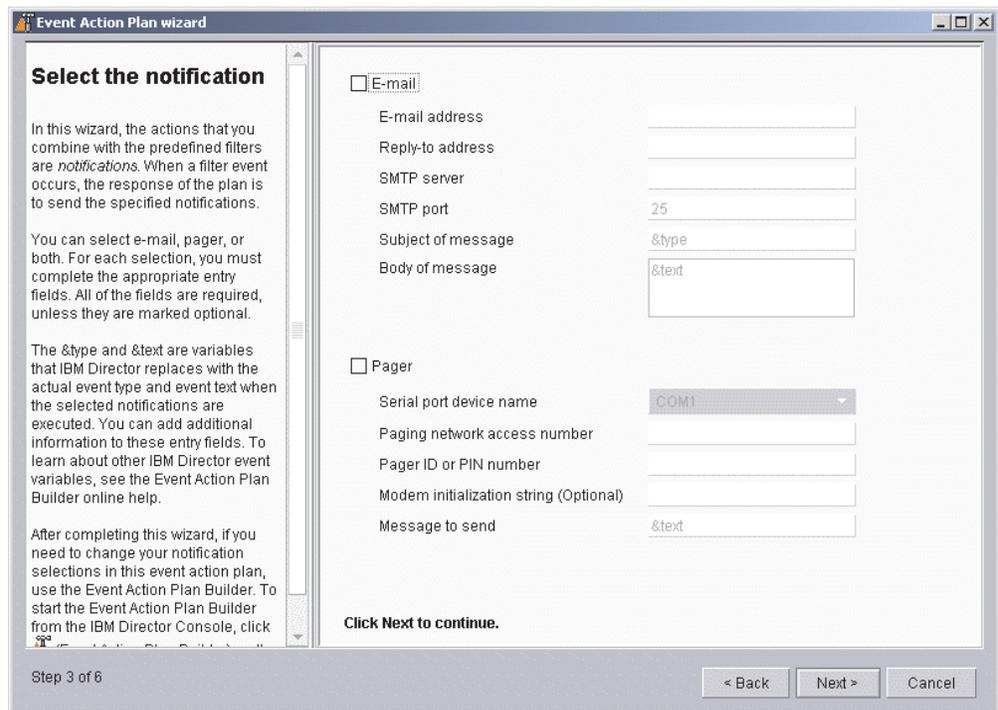


Figure 40. Event Action Plan wizard: “Select the notification” window

5. If you want to be notified by e-mail when an event occurs, select the **E-mail** check box. Then, configure the e-mail notification:
  - a. In the **E-mail address** field, type the e-mail address to which the notification will be sent.
  - b. In the **Reply-to address** field, type the e-mail address that will be displayed in the reply-to field of the e-mail.

- c. In the **SMTP server** field, type the host name or IP address of the Simple Mail Transfer Protocol (SMTP) server.
- d. In the **SMTP port** field, type the port number of the SMTP server. By default, the SMTP port is set to 25.
- e. In the **Subject of message** field, type the message that will be displayed in the subject-line of the e-mail. By default, this is set to &type.

You can add additional information to the entry field. For example, you might want to type the following string:

```
IBM Director alert: &system &type
```

When the e-mail is generated, the name of the managed system is substituted for &system, and the type of event that occurred is substituted for &type.

- f. In the **Body of message** field, type the message that will be displayed in the body of the e-mail. By default, this is set to &text.

You can add additional information to the entry field. For example, you might want to type the following string:

```
&time &date &text
```

When the e-mail is generated, the body will contain the time and date the event occurred, as well as details about the event.

**Note:** &type, &system, &time, &date, and &text are event-data substitution variables. For information about other event-data substitution variables, see the *IBM Director 4.20 Systems Management Guide*.

6. If you want to be notified by pager, select the **Pager** check box. Then, configure the pager notification:
  - a. From the **Serial port device name** list, select the name of the serial port device.
  - b. In the **Paging network access number** field, type the telephone number that will be dialed when an event occurs.
  - c. In the **Pager ID or PIN** field, type the pager ID or personal identification number (PIN).
  - d. In the **Modem initialization string (Optional)** field, type the modem initialization string.
  - e. In the **Message to send** field, type the message that will be sent when an event occurs.
7. Click **Next**. The “Apply the event action plan” window opens.

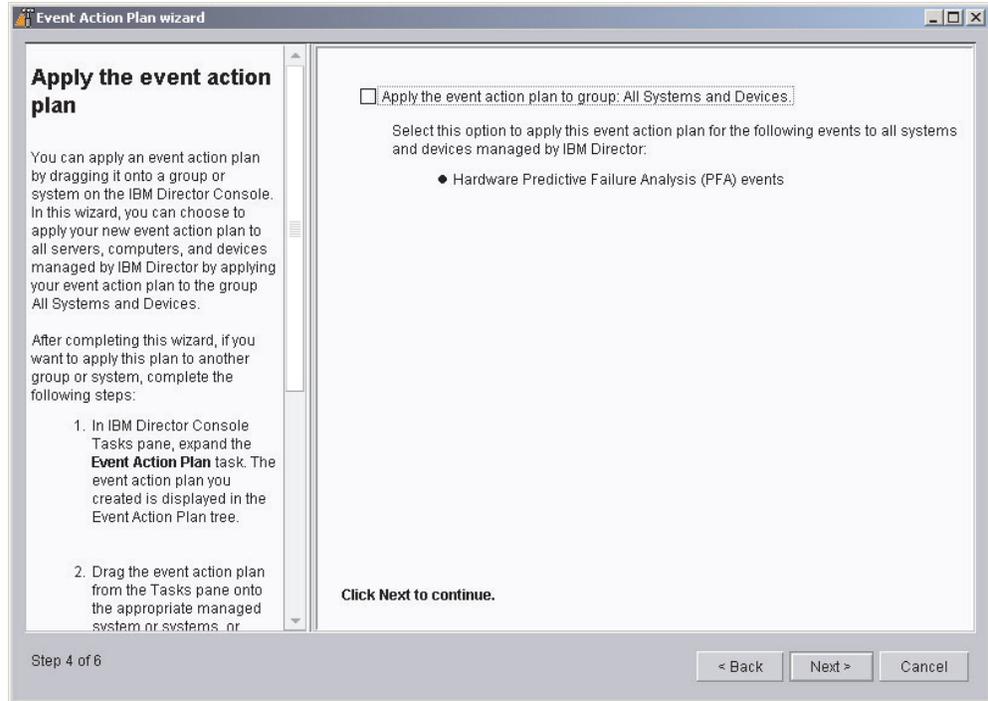


Figure 41. Event Action Plan wizard: “Apply the event action plan” window

8. If you want to apply the event action plan to all systems in the IBM Director environment, select the **Apply event action plan to group: All Systems and Devices** check box.
9. Click **Next**. The “Discover all systems and devices” window opens.

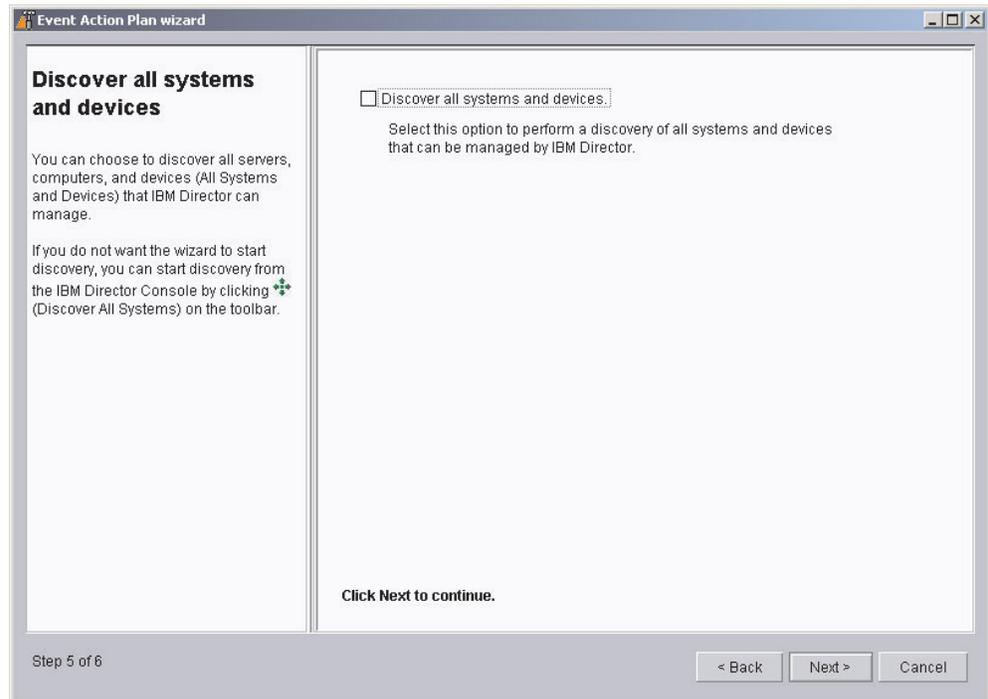


Figure 42. Event Action Plan wizard: “Discover all systems and devices” window

10. If you want IBM Director Server to discover all the managed systems and SNMP devices on the network, select the **Discover all systems and devices** check box.
11. Click **Next**. The “Review your selection summary” window opens. Review the selections. If you want to change any of your selections, click

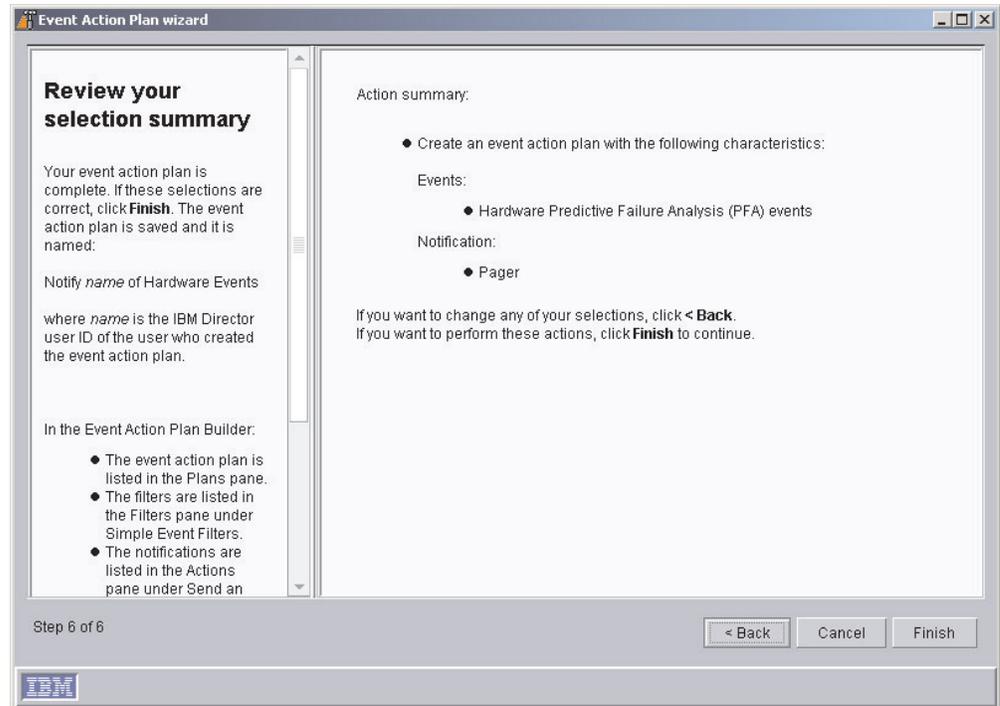


Figure 43. Event Action Plan wizard: “Review your selection summary” window

### Back.

12. Click **Finish**. The event action plan is saved. It is named “Notify *name* of Hardware Events,” where *name* is the IBM Director user ID of the user who created the event action plan.

---

## Discovering managed systems, devices, and objects

Discovery is the process by which IBM Director Server identifies and establishes connections with systems on which IBM Director Agent is installed. The management server sends out a discovery request and waits for responses from managed systems. The managed systems listen for this request and respond to the management server that sent the request.

**Note:** (Windows 2000, Server Edition only) The initial discovery performed by the management server is resource intensive. After the initial discovery is completed, the resource utilization returns to normal.

## Types of discovery

IBM Director supports four types of discovery concerning managed systems and SNMP devices:

### **Broadcast discovery**

Broadcast discovery sends out a general broadcast packet over the LAN. The destination address of this packet depends on the particular protocol used to communicate with the managed systems.

Broadcast discovery also can send out a broadcast packet to specific subnets. If you specify the IP address and subnet mask for a system (a discovery seed address), IBM Director sends a broadcast packet to that specific subnet and discovers all managed systems on that subnet that do not filter out broadcast packets.

### **Multicast discovery**

Multicast discovery operates by sending a packet to the multicast address. By default, IBM Director uses 224.0.1.118 as the multicast address. Managed systems monitor this address and respond to the multicast from the management server. Multicasts are defined with maximum time to live (TTL), which is the number of times a packet is passed between subnets. After the TTL expires, the packet is discarded.

Multicasts are useful for networks that filter broadcasts but do not filter multicasts. Multicast discovery is available only for TCP/IP systems.

### **Unicast discovery**

Unicast discovery sends a directed request to a specific address or range of addresses. This method generates a discovery request for each address in the range, but it is useful in networks where both broadcasts and multicasts are filtered. Unicast discovery is available only for TCP/IP systems.

### **Broadcast relay agents**

Broadcast relay enables the server to discover TCP/IP and IPX systems when the systems are not directly reachable by broadcast packets because of network configuration. This situation can occur in networks where the management server and managed systems are in separate subnets and the network between them does not allow broadcast packets to pass from one subnet to the other.

This option generates less network traffic than unicast discovery and avoids many of the problems associated with filtered broadcasts. In broadcast relay, the management server sends a special discovery request message to a particular managed system, instructing the managed system to perform a discovery on the local subnet using a general broadcast. When managed systems on that subnet receive the discovery request, they reply to the management server that made the original request.

The management server performs all types of discovery simultaneously.

## Setting discovery preferences

Complete the following steps to configure discovery preferences:

1. From IBM Director Console, click **Options** → **Discovery Preferences**. The “Discovery Preferences” window opens.

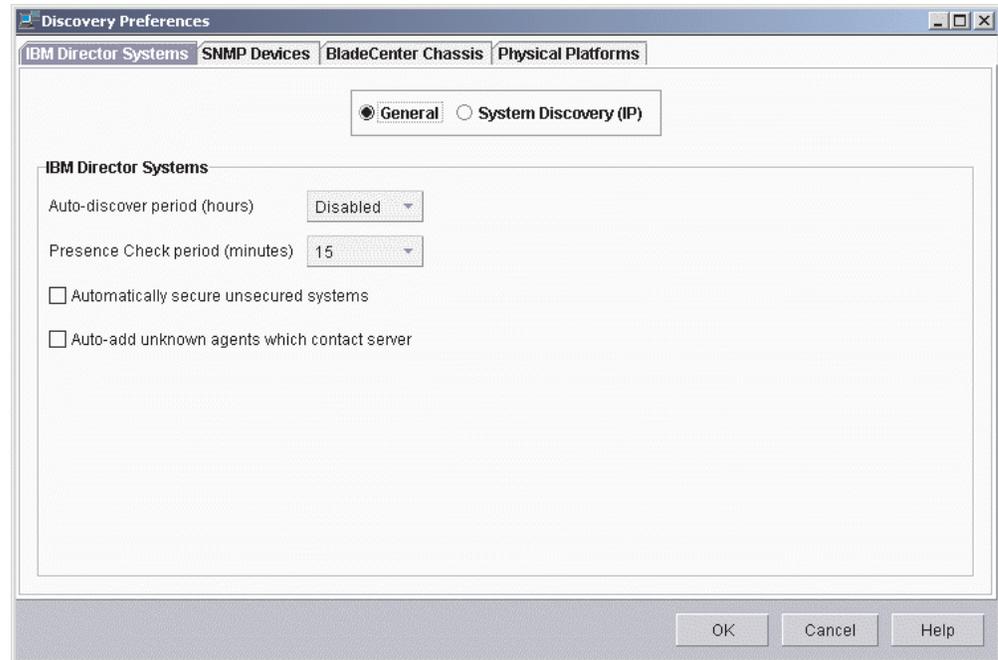


Figure 44. “Discovery Preferences” window

This window has four pages:

### **IBM Director Systems**

Sets general discovery preferences and defines how IBM Director discovers managed systems reachable through TCP/IP

### **SNMP Discovery**

Defines how IBM Director discovers SNMP devices

### **BladeCenter Chassis**

Sets general discovery preferences for BladeCenter chassis

### **Physical Platforms**

Sets general discovery preferences for physical platforms

2. To move from one page to another, click the applicable tab. Click **OK** when you have finished configuring discovery preferences.

## Discovering service processors

While IBM Director automatically discovers and creates physical platform managed objects (PPMOs) for Remote Supervisor Adapters and Remote Supervisor Adapter IIs, IBM Director only discovers the following service processors when they are installed in servers on which IBM Director Agent is installed:

- ASM PCI Adapter
- ASM processor
- IPMI baseboard management controller
- ISMP

In addition, if you add an optional service processor to a server that contains an ASM processor, you must manually create a management processor object for the optional service processor.

## Manually creating a management processor object

When you add an ASM PCI Adapter, a Remote Supervisor Adapter, or a Remote Supervisor Adapter II to a server with an ASM processor, you must manually create a management processor object for the optional service processor. IBM Director Server does not discover the optional service processor nor does it create a physical platform managed object (PPMO) automatically.

For IBM Director to manage an optional service processor, you must create a management processor object manually. After you create a management processor object, you can perform the following tasks:

- Configure the ASM PCI Adapter, Remote Supervisor Adapter, or Remote Supervisor Adapter II using the Management Processor Assistant task
- (If the optional service processor acts as a gateway service processor) Use out-of-band management to manage the service processors on the ASM interconnect network

Complete the following steps to create a management processor object manually:

1. Start IBM Director Console.
2. Right-click in the Group Contents pane; then, click **New → Management Processors**. The “Add Management Processors” window opens.

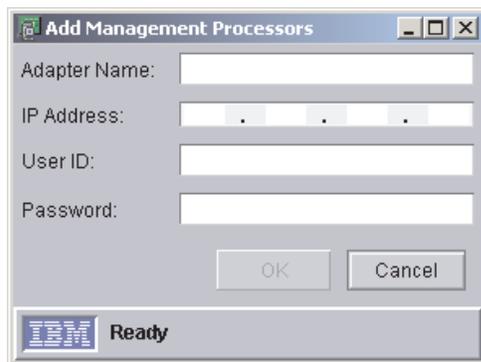


Figure 45. “Add Management Processors” window

3. In the **Adapter Name** field, type a name for the service processor.

**Note:** A best practice is assign the service processor a name that clearly identifies the service processor type and the server that it manages, for example, SystemName-ServiceProcessorType.

4. In the **IP Address** field, type the IP address of the service processor.
5. In the **User ID** field, type a valid user ID for the service processor.
6. In the **Password** field, type the password that corresponds to the user ID you typed in step 5.
7. Click **OK**.
8. The management processor object is displayed in the Group Contents pane.

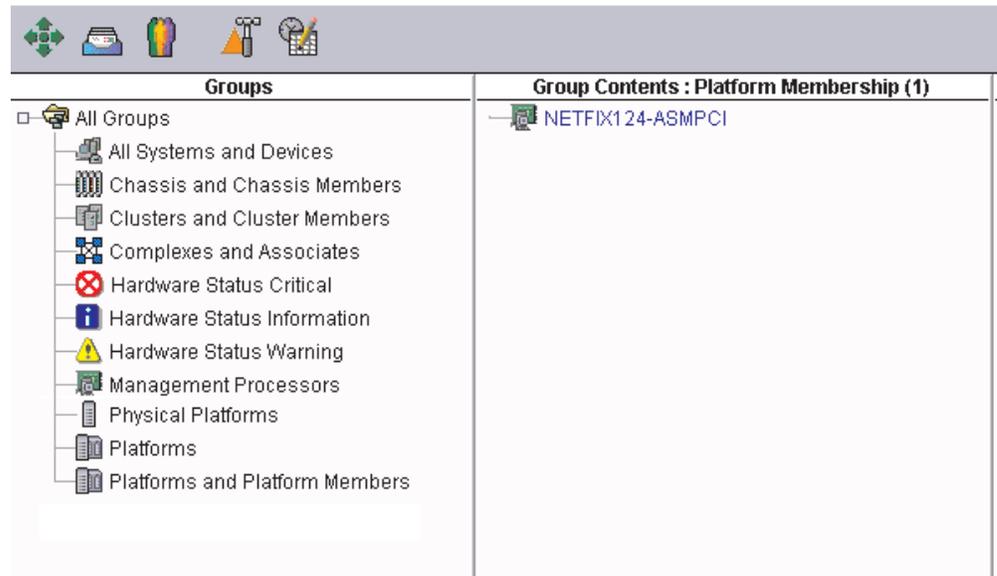


Figure 46. IBM Director Console: Group Contents pane

## Authorizing IBM Director users

IBM Director Console uses the operating-system user accounts for user-logout security. When a user logs in to IBM Director, the user ID and password verification process used by the operating system is used to validate the user's authority to access IBM Director.

To use IBM Director, a user must have an operating-system account on the management server or the domain. In addition, a user must meet one of the following requirements, depending on the operating system running on the management server:

<b>For i5/OS</b>	Member of the IBM Director Administrators or IBM Director Super Administrators group
<b>For Linux</b>	Member of the diradmin or dirsuper group
<b>For Windows</b>	One of the following criteria: <ul style="list-style-type: none"> <li>• Member of the DirAdmin or DirSuper group</li> <li>• Administrator privileges on the management server or the domain</li> </ul>

Users' ability to perform tasks depends on which access privileges they have been assigned in the IBM Director environment. A super user can configure a default set of privileges for the administrator group. A super user also can edit user accounts on an individual basis.

## Creating user-account defaults

A super user can use the User Defaults Editor to set the default access privileges for new members of the administrators group. Complete the following steps to create user-account defaults:

1. In IBM Director Console, click **Options** → **User Administration**. The "User Administration" window opens.

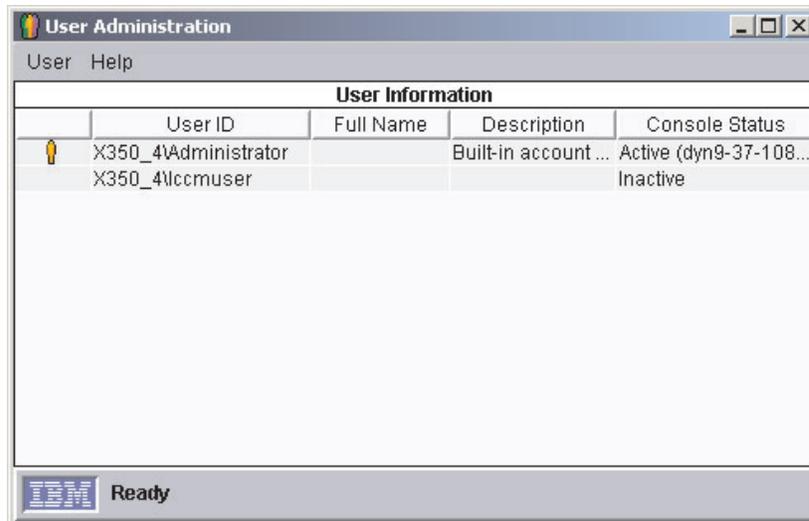


Figure 47. "User Administration" window

This window contains a list of all users authorized to access IBM Director.

2. Click **User** → **User Defaults**. The "User Defaults Editor" window opens.

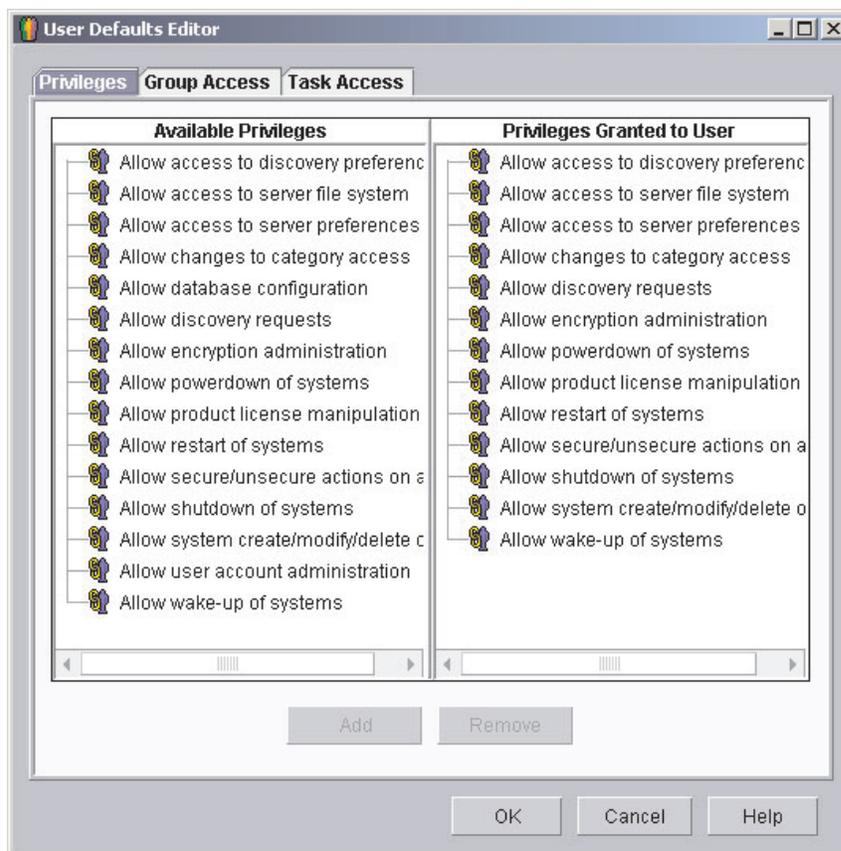


Figure 48. "User Defaults Editor" window

From this window, you can set the default access privileges for new members of the DirAdmin group.

**Notes:**

- a. For increased security, consider removing all default access privileges. You will have to set access levels for each user, but you can be sure that a user will not accidentally get access to restricted groups or tasks.
- b. You can restrict access to the Event Action Plan wizard by removing users' access to the Event Action Plan Builder task.

## Editing an individual user's access privileges

Complete the following steps to edit a user's access privileges:

- 1. In IBM Director Console, click **Options** → **User Administration**. The "User Administration" window opens.

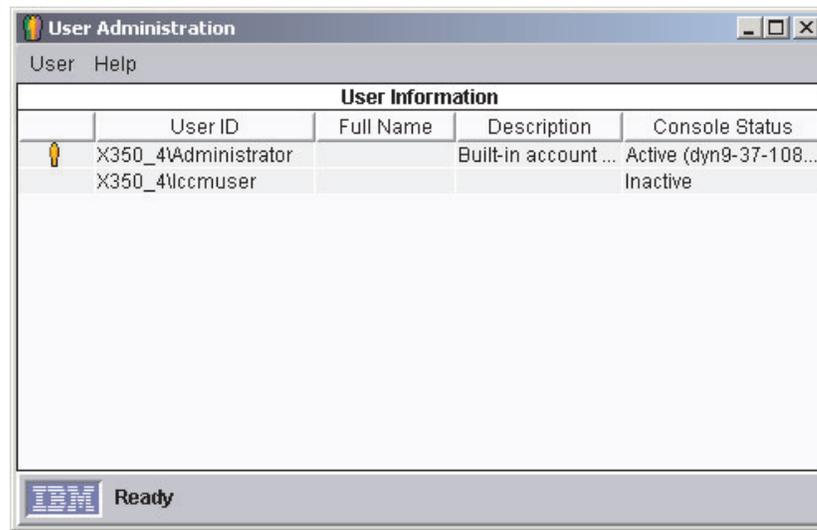


Figure 49. "User Administration" window

This window contains a list of all users authorized to access IBM Director.

- 2. Select the user whose access privileges you want to modify. Click **User** → **Edit**. The "User Editor" window opens.

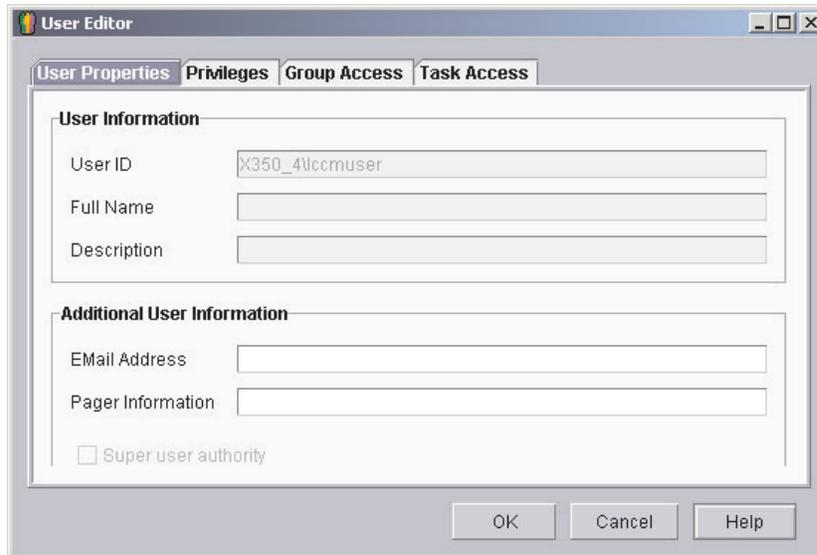


Figure 50. "User Editor" window: "User Properties" page

3. Click the **Privileges** tab. The "Privileges" page is displayed.

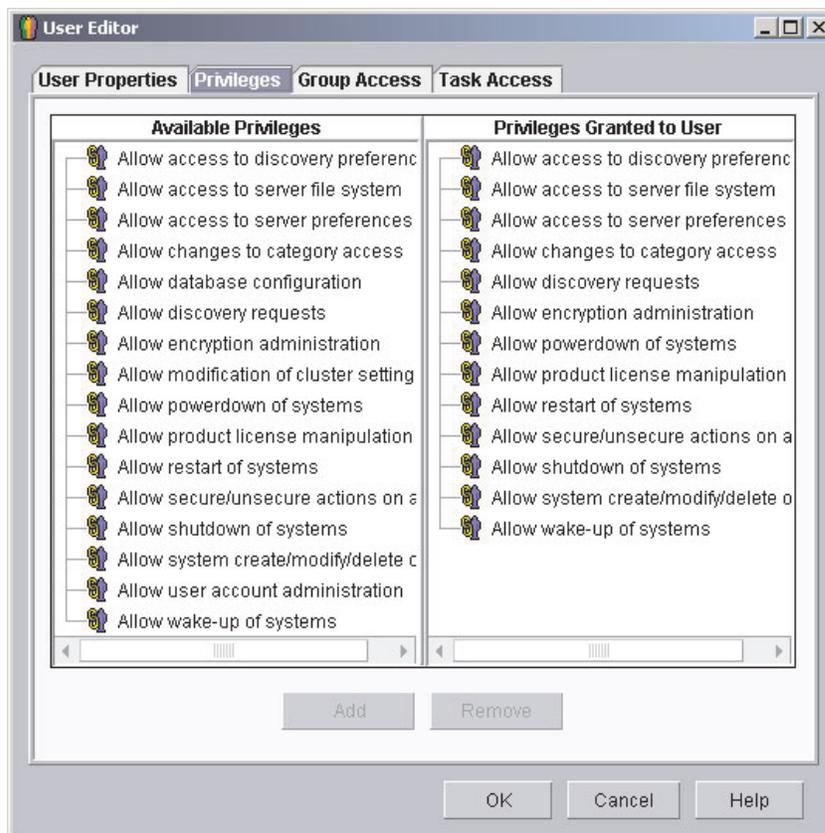


Figure 51. "User Editor" window: "Privileges" page

4. To add a privilege, click the privilege in the **Available Privileges** pane and then click **Add**. To remove a privilege, click the privilege in the **Privileges Granted to User** pane and then click **Remove**.
5. To restrict the user's access to groups, click the **Group Access** tab. The "Group Access" page is displayed.

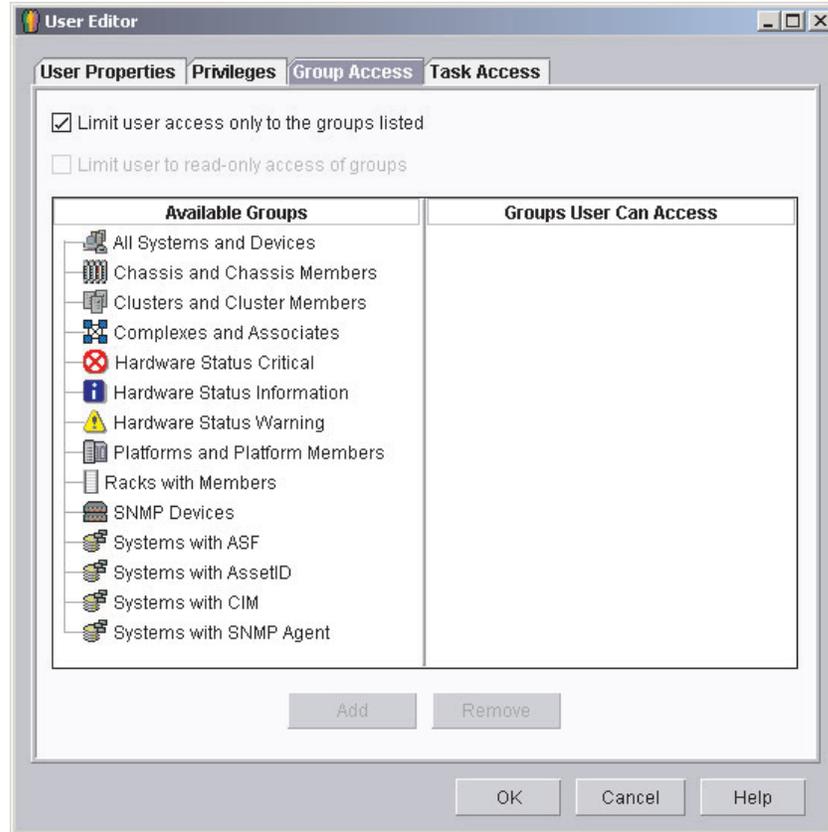


Figure 52. "User Editor" window: "Group Access" page

6. To permit the user to access specific groups only, select the **Limit user access only to the groups listed** check box. To add a group, click the group in the **Available Groups** pane and click **Add**. To remove a group, click the group in the **Groups User Can Access** pane and click **Remove**.  
To prevent the user from creating new groups or modifying existing groups, select the **Limit user to read-only access of groups** check box.

7. To restrict the user's access to tasks, click the **Task Access** tab. The "Task Access" page is displayed.

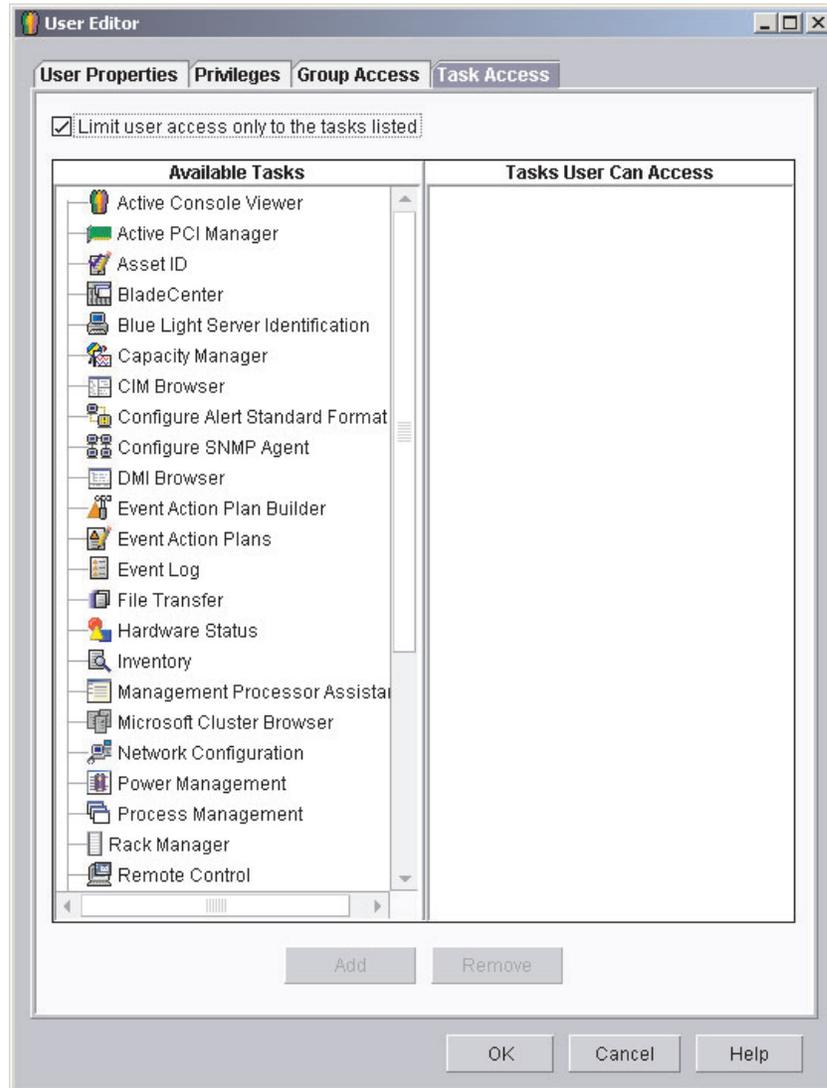


Figure 53. "User Editor" window: "Task Access" page

8. To restrict the user to performing certain tasks only, select the **Limit user access only to the tasks listed** check box. To add a task, click the task in the **Available Tasks** pane and click **Add**. To remove a task, click the task in the **Tasks User Can Access** pane and click **Remove**.

**Note:** You can restrict access to the Event Action Plan wizard by removing the user's access to the Event Action Plan Builder task.

9. When you have finished editing the user's privileges, click **OK**. The "User Editor" window closes.

---

## Configuring security settings

This section contains information about assigning digital certificates, enabling Secure Sockets Layer (SSL), and restricting IBM Director Console sessions to particular ports and session keys. It also includes information about configuring a custom access policy for Web-based Access.

### Assigning digital certificates (i5/OS only)

You must use option 34, OS/400 - Digital Certificate Manager to assign a digital certificate before you enable SSL. Use the default server certificate in the \*SYSTEM certificate store of Digital Certificate Manager.

For more information, see the Digital Certificate Manager documentation on the IBM @server iSeries Information Center Web site at <http://www.ibm.com/servers/eserver/series/infocenter>.

### Enabling SSL

**Note:** If you enable SSL, you cannot use Web-based Access to view hardware status information about the management server.

To enable SSL between a management server and a management console, you must modify the TWGServer.prop and TWGConsole.prop files located on each system. If you installed IBM Director Server and IBM Director Console in the default location, these files are located in the following directories:

<b>For i5/OS</b>	/QIBM/UserData/Director/data/
<b>For Linux</b>	/opt/IBM/director/data/
<b>For Windows</b>	d:\Program Files\IBM\Director\data

where *d* is the drive letter of the hard disk on which IBM Director is installed.

Complete the following steps to enable SSL between a management server and management console:

1. Using an ASCII text editor or the OS/400 Edit File (EDTF) command, open the TWGServer.prop file located on the management server.
2. To enable SSL for data transmitted between IBM Director Server and IBM Director Console, add the following line:  
`twg.gateway.link.1=com.tivoli.twg.libs.TWGSSLLink`
3. To enable SSL for DIRCMD sessions, add one of the following statements:

<b>To permit access only through SSL</b>	<code>twg.cli.gateway.link.1=com.tivoli.twg.libs.TWGSSLLink</code> <code>twg.cli.gateway.link.1.initparam=PortNumber</code>
<b>To permit access either through clear text or SSL</b>	<code>twg.cli.gateway.link.2=com.tivoli.twg.libs.TWGSSLLink</code> <code>twg.cli.gateway.link.2.initparam=PortNumber</code>

where *PortNumber* is the port.

4. Save and close the TWGServer.prop file.
5. Stop and restart IBM Director Server.

**Note:** (Management server running i5/OS) If a digital certificate has not been assigned, IBM Director Server will not restart.

6. Using an ASCII text editor or the OS/400 Edit File (EDTF) command, open the TWGConsole.prop file located on the management console.
7. Modify the value of twg.gateway.link.1 to read as follows:  
twg.gateway.link.1=com.tivoli.twg.libs.TWGSSLLink
8. Add the same statements that you added to the TWGServer.prop file in step 3 on page 103.
9. Save and close the TWGConsole.prop file.
10. Stop and restart IBM Director Console.

By default, all supported cipher suites are enabled. See “Secure Sockets Layer (SSL)” on page 34 for a list of the supported cipher suites.

## Restricting IBM Director Console sessions

You can further modify the TWGServer.prop and TWGConsole.prop files to specify the port used by IBM Director Console sessions and the specific cipher suites to be used. If you installed IBM Director Server and IBM Director Console in the default location, these files are located in the following directories on the management server and management console:

<b>For i5/OS</b>	/QIBM/UserData/Director/data/
<b>For Linux</b>	/opt/IBM/director/data/
<b>For Windows</b>	d:\Program Files\IBM\Director\data

where *d* is the drive letter of the hard disk on which IBM Director is installed.

Complete the following steps:

1. Using an ASCII text editor or the OS/400 Edit File (EDTF) command, open the TWGServer.prop file.
2. Modify the file so that it contains the following properties:

```
twg.gateway.link.1=com.tivoli.twg.libs.TWGSSLLink
twg.gateway.link.1.initparm=PortNumber -cipherSuites CipherSuite
```

where *PortNumber* is the port and *CipherSuite* is the cipher suite.

**Note:** Separate multiple cipher suites by a comma; do not add a space after the comma.

3. Save and close the TWGServer.prop file.
4. Stop and restart IBM Director Server.

**Note:** (Management server running i5/OS) If a digital certificate has not been assigned, IBM Director Server will not restart.

5. Using an ASCII text editor or the OS/400 Edit File (EDTF) command, open TWGConsole.prop file.
6. Modify the TWGConsole.prop file so that it contains the same properties as the TWGServer.prop file that you modified in step 2.
7. Save and close the TWGConsole.prop file.
8. Stop and restart IBM Director Console.

9. (Management servers running Linux or Windows) Copy a cacerts.ssl file to the following directory on the management server:

<b>For Linux</b>	/opt/IBM/director/data
<b>For Windows</b>	d:\Program Files\IBM\director\data

You can find an existing cacerts.ssl file in the following directory:

<b>For Linux</b>	/opt/IBM/director/jre/lib/security
<b>For Windows</b>	d:\Program Files\IBM\director\jre\lib\security

10. Import the applicable RSA or Secure Hash Algorithm (SHA) certificate into the cacerts.ssl file. You can use the keytool program located in the following directory:

<b>For Linux</b>	/opt/IBM/director/data
<b>For Windows</b>	d:\Program Files\IBM\director\data

To establish an SSL session without importing an RSA or SHA certificate, use an anonymous cipher suite.

**Note:** Management servers running i5/OS do not support anonymous cipher suites.

## Configuring a custom access policy for Web-based Access (Windows only)

If IBM Director Agent is installed on a Windows NT file system (NTFS) partition, you can configure a custom access policy for Web-based Access.

**Note:** Windows XP might hide the file permission editor. You must enable editing of file permissions before you can modify the access policy.

Complete the following steps to customize the access policy:

1. Using Windows Explorer, select the admin4.txt file. If you installed IBM Director Agent in the default location, this file is located in the Program Files\IBM\Director\websrv\cgi-bin directory.
2. Edit the file access permissions. Grant read access to this file for users and groups that you want to be able to modify system settings.
3. Using Windows Explorer, select the user1.txt file. If you installed IBM Director Agent in the default location, this file is located in the Program Files\IBM\Director\websrv\cgi-bin directory.
4. Edit the file access permissions. Grant read access to this file for users and groups that you want to be able to view but not modify the system settings

**Note:** Do *not* delete the admin4.txt and user1.txt files to restrict all Web-based Access to the managed system. Instead, remove the read-only permissions for administrators and users, and leave the files in the Program Files\IBM\Director\websrv\cgi-bin directory.

---

## Configuring software distribution

You can use the IBM Director Software Distribution task to import IBM software, build software packages, and distribute the packages to managed systems.

If you purchase and install IBM Director 4.1 Software Distribution (Premium Edition), you have additional capabilities. You can accomplish the following additional tasks:

- Import non-IBM software and build software packages using the following wizards:
  - AIX InstallIP wizard (AIX)
  - InstallShield Package wizard (Windows)
  - Microsoft Windows Installer wizard (Windows)
  - OS/400 Restore Library Package wizard (i5/OS)
  - OS/400 Restore Licensed Program Package wizard (i5/OS)
  - OS/400 Restore Object Package wizard (i5/OS)
  - RPM Package wizard (AIX and Linux)
- Import IBM or non-IBM software and build a software package using the Custom Package Editor
- Back up or export a software package
- Import a software package created by another management server, using the Director File Package wizard

**Note:** Managed systems running NetWare do not support the IBM Director Software Distribution task.

## Methods of software distribution

IBM Director supports the following methods of software distribution:

- Streaming from the management server
- Redirected distribution

### Streaming from the management server

Software-distribution packages are copied directly from the management server to the managed system.

This method of software distribution is resource-intensive. It can have a negative effect on the management server performance. In addition, a package distributed by this method requires that the target managed system has empty disk space twice the size of the package.

Streaming from the management server has one advantage, however. If a network connection is broken during the transmission, IBM Director attempts to resume the connection from the point at which the transmission was interrupted. If the streaming operation can be resumed, retransmission time is saved.

Because of the potential to resume distribution, you might prefer to stream a software package from the management server if you have an unreliable or slow network link.

### Redirected distribution

Many software packages are tens or hundreds of megabytes in size. Distributing software of this size across a large network can cause bottlenecks in network data transmission. To avoid this problem, you can set up a universal naming convention

(UNC) or FTP share on a network server. IBM Director Server streams software packages to the network share, where they are cached. From the share, they are either streamed to the managed systems or, in the case of software that uses the Microsoft Windows Installer or InstallShield as the installation utility, installed directly from the file-distribution server.

Redirected distribution greatly reduces the software-distribution traffic in your network. It uses fewer management server system resources. In addition, if you install InstallShield or Microsoft Windows Installer (MSI) packages directly from the file-distribution server, redirected distribution requires less disk space on the managed systems.

Redirected distribution has one limitation: if a redirected distribution of a software package is interrupted (for example, if the network connection is lost), the installation must begin all over.

## Setting up file-distribution servers

IBM Director supports UNC-based and FTP-based file distribution software. See your server documentation for information about setting up a shared subdirectory.

**Note:** You do not need to install IBM Director on the file-distribution server.

### File-distribution server considerations

Consider the following issues when setting up file-distribution shares:

- In a Windows environment, the file-distribution server must either be a member of the same domain as the management server or have a trust relationship with that domain.
- The management server must have full read/write access to the share. Otherwise, software distribution defaults to streaming from the management server.
- The share must allow read access to all managed systems that you want to access the share.
- If the file-distribution server is configured as an FTP server, you can select to use FTP when transferring packages from the management server to the share. For managed systems running Windows, the home directory for the FTP login must be the same directory as the file-distribution server. For example, if `c:\stuff\swd_share` is mapped to `\\server\swd_share`, then `c:\stuff\swd_share` must be the home directory for the FTP user ID login used on the FTP file-distribution server configuration screen.
- If you want managed systems to use null credentials to access the share, you must issue the **twgshare** command. This alters a registry setting on the file-distribution server, which enables managed systems to use null credentials to access the share. To issue the **twgshare** command, complete the following steps:
  1. Copy the `twgshare.exe` file to the file-distribution server. This file is in the `\IBM\director\bin\` directory.
  2. From a command prompt, type the following command:

```
twgshare -a sharename
```

where *sharename* is the name of the share on the file-distribution server.
- If you do not want to use null credentials (which are a security risk), you must set up an operating-system account on the file-distribution server. Use the user ID

and password for this account when you configure distribution preferences for managed systems. See “Configuring distribution preferences for managed systems” on page 110.

## Configuring IBM Director to use a file-distribution server

Complete the following steps to configure IBM Director Server to use a file-distribution server:

1. Start IBM Director Console.
2. Click **Options** → **Server Preferences**. The “Server Preferences” window opens.
3. Click the **File Distribution Server** tab. A list is displayed of all configured file-distribution servers.
4. Click **Add**. The “Add Share Name” window opens.

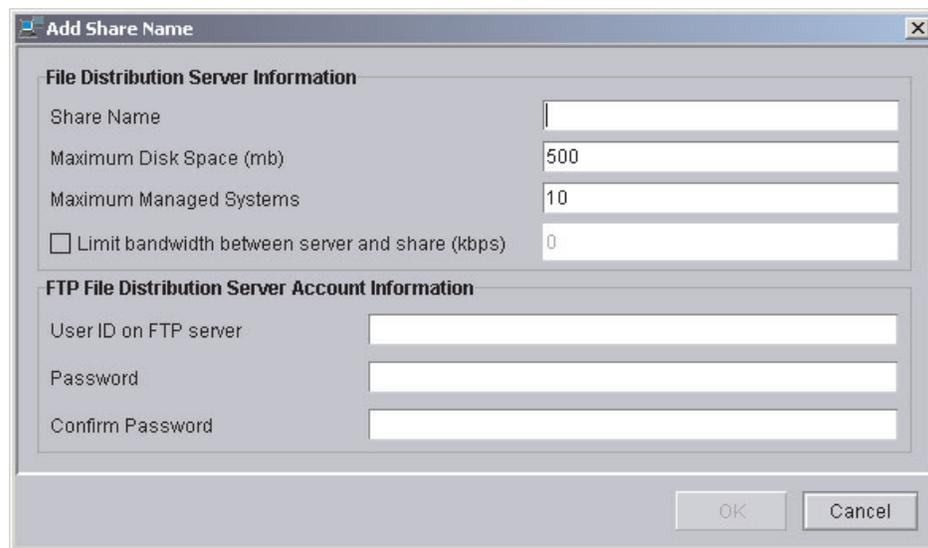


Figure 54. IBM Director Console: “Add Share Name” window

5. In the **Share Name** field, type the name of the file-distribution server using UNC notation. To specify FTP as the transport protocol, begin the share-name entry with ftp:, for example ftp:\\ServerName\\AccountName.
6. In the **Maximum Disk Space** field, type the maximum amount of disk space (in MB) that can be allocated on the file-distribution server for software distribution.
7. In the **Maximum Managed Systems** field, type the maximum number of managed systems that can receive a software package at the same time.
8. To limit the bandwidth that can be used to send packages between IBM Director Server and the file-distribution server, select the **Limit bandwidth between server and share (kbps)** check box. In the entry field, type the maximum bandwidth, in kilobytes per second (KBps), that can be used to send packages between IBM Director and the file-distribution server.

**Note:** You might want to limit the bandwidth when a dedicated connection, such as integrated services digital network (ISDN), is used for copying the files from IBM Director Server to the share.

9. If you specified an FTP-based server in step 5 on page 108, you must provide information about the FTP server:
  - a. In the **User ID on FTP server** field, type a user ID authorized to access the FTP server installed on the share.
  - b. In the **Password** field, type the password associated with the user ID.
  - c. In the **Confirm password** field, retype the password associated with the user ID.
10. Press **OK**. The “Server Preferences” window reopens. The data you entered in the “Add Share” window is displayed.

If you have multiple file-distribution servers, repeat this procedure for each server.

## Configuring software-distribution preferences

Complete the following steps to configure software-distribution preferences:

1. If necessary, start IBM Director Console.
2. Click **Options** → **Server Preferences**. The “Server Preferences” window opens.
3. Click the **Software Distribution** tab. The “Software Distribution” page is displayed.

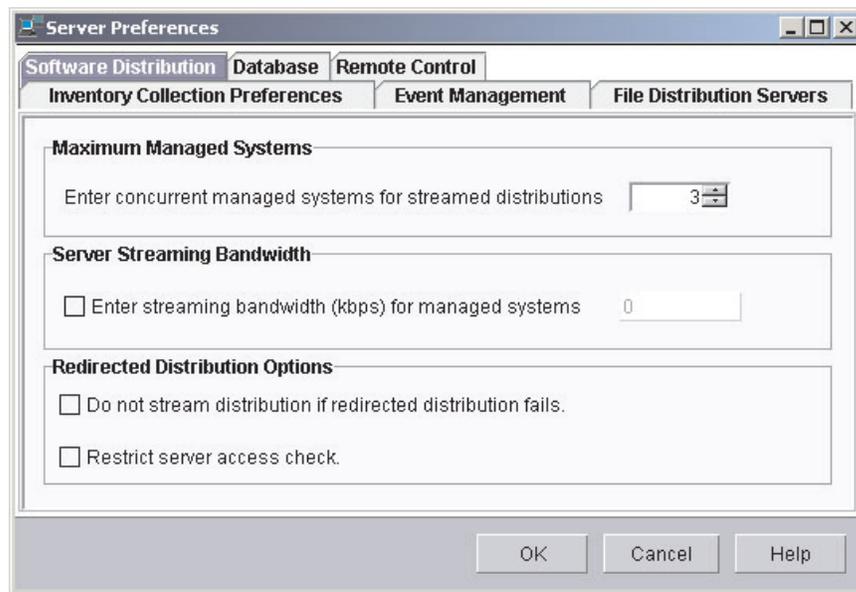


Figure 55. IBM Director Console: “Software Distribution” page

4. In the **Maximum Managed Systems** field, type the maximum number of managed systems to which IBM Director Server can concurrently stream software packages. (The default value is three.)
5. To limit the bandwidth used to stream packages, select the **Enter streaming bandwidth (kbps) for managed systems** check box. In the entry field, type the bandwidth, in kilobytes per second (KBps), used to stream packages from either IBM Director Server or a file-distribution server to the managed system.

**Note:** To specify values less than 1 KBps, type a decimal. The minimum acceptable value is 0.25 (256 bytes per second).

6. To avoid streaming a package in the event that a redirected distribution fails, select the **Do not stream distribution if redirected distribution fails** check box.

7. To prevent IBM Director Server from performing an access check of *all* of the file-distribution shares, select the **Restrict server access check** check box. This restricts the access check to *only* the file-distribution shares you configure for a specific managed system or group. See “Configuring distribution preferences for managed systems” for more information about restricting access to specific file-distribution shares.
8. Click **OK**.

## Configuring distribution preferences for managed systems

After you configure IBM Director to use a file-distribution server, you can assign unique policies to a managed system and groups. By default, a managed system attempts to access all shares that have been defined to the management server. You can configure the following software-distribution preferences for a managed system or group:

- Restrict access to specific shares
- Specify whether software distribution occurs through streaming or redirected distribution
- Limit the bandwidth used for software distribution

Complete the following steps to define distribution preferences:

1. If necessary, start IBM Director Console.
2. In the Group Contents pane, right-click the managed system or group.
3. Click **Distribution Preferences**. The “Distribution Preferences” window opens.

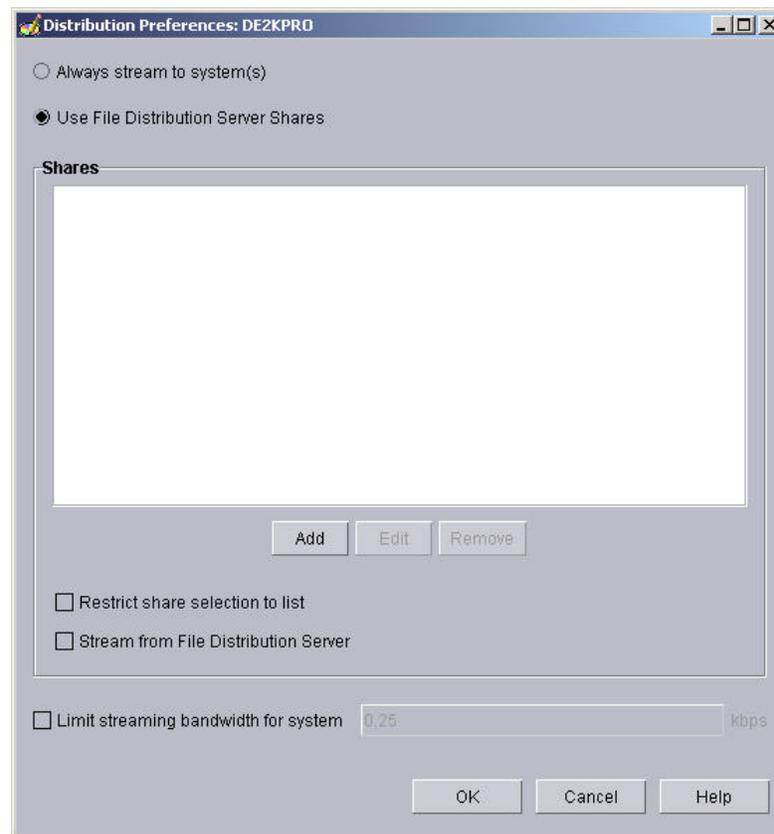


Figure 56. IBM Director Console: “Managed System Distribution Preferences” window

4. Select the method of software distribution:
  - If you want to copy packages directly from IBM Director Server to the managed system or group, click **Always stream to the Managed System(s)**.
  - If you want to copy packages from a share to the managed system or group, click **Use File Distribution Server Shares**.
5. To add a share, click **Add**. The “Add Share Name” window opens.

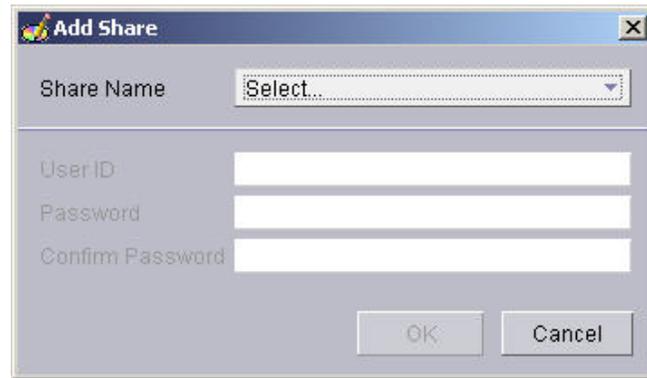


Figure 57. IBM Director Console: “Add Share Name” window

In the **Share Name** field, select the share. If necessary, specify a user ID and password for an account that can access the share.

Click **OK**.

6. Repeat step 5 until you have added all the shares that you want the managed system or group to access.
7. If you want to limit the shares that the managed system or group can access to only those displayed, select the **Restrict share selection to list** check box.

**Note:** If you do not select this option, other defined shares can be used for software distribution if the shares displayed are not available. In this situation, UNC-based shares are accessed using null credentials and FTP-based shares are accessed anonymously.

8. To ensure that software packages are always streamed rather than installed remotely, select the **Stream from File Distribution Server** check box.

**Note:** Software packages that contain applications that use Microsoft Windows Installer (MSI) or InstallShield as their installation mechanism are installed directly from the file-distribution share *unless* the **Stream from File Distribution Server** check box is selected.

9. To limit the bandwidth that is used when copying packages from the file-distribution server to the managed system or group, select the **Limit streaming bandwidth for system** check box. In the entry field, type the bandwidth, in kilobytes per second (KBps), that is used for copying packages to the managed system or group. This value also determines the bandwidth that is used to copy packages from IBM Director Server and the managed system or group.



---

## Chapter 8. Configuring an IBM BladeCenter chassis

This chapter contains information about discovering and configuring an IBM BladeCenter chassis. It also includes information about creating a chassis detect-and-deploy profile.

You can use the BladeCenter Deployment wizard to configure the BladeCenter chassis. If Remote Deployment Manager (RDM) is installed on your management server, you also can use the wizard to install operating systems and IBM Director Agent on the blade servers.

You also can use the BladeCenter Assistant task to configure the BladeCenter chassis. See the *IBM Director 4.20 Systems Management Guide* for more information.

**Note:** After configuring the BladeCenter chassis, avoid changing the database application that is used with IBM Director Server. Doing so will cause inventory errors.

---

### Discovering a BladeCenter chassis

Before you can configure the BladeCenter chassis, IBM Director must discover the BladeCenter chassis.

IBM Director communicates with the BladeCenter chassis through the external Ethernet port on the BladeCenter management module. When the BladeCenter management module is first started, the management module attempts to acquire an IP address for the external management port using DHCP. If this attempt fails, the BladeCenter management module assigns an IP address (192.168.70.125) to the external management port.

**Note:** If you do not use a DHCP server to assign a temporary IP address to the BladeCenter chassis, introduce only *one* BladeCenter chassis onto the network at a time. IBM Director must discover and configure the chassis before another chassis is added to the LAN. Otherwise, an IP address conflict will occur.

If the management server and the BladeCenter chassis are on the same subnet, IBM Director can discover the BladeCenter chassis automatically. Go to “Automatically discovering the BladeCenter chassis” on page 114.

If the management server and the BladeCenter chassis are not on the same subnet, you must discover the BladeCenter chassis manually. Go to “Manually discovering the BladeCenter chassis” on page 114.

## Automatically discovering the BladeCenter chassis

IBM Director uses the Service Location Protocol (SLP) to discover the BladeCenter chassis. The management server and the BladeCenter chassis must be connected to the network and on the same subnet. One of the following conditions must be true:

- The network contains a DHCP server that has assigned an IP address to the management module.
- You manually changed the default IP address of the management module to a valid IP address on the same subnet as the management server. See “Manually changing the IP address of the BladeCenter chassis” on page 115 for more information.

Complete the following steps to discover the BladeCenter chassis:

1. Start IBM Director Console.
2. Click **Tasks** → **Discover Systems** → **BladeCenter Chassis**. The discovery operation begins. When it is completed, the BladeCenter chassis managed object is displayed in the Group Contents pane.

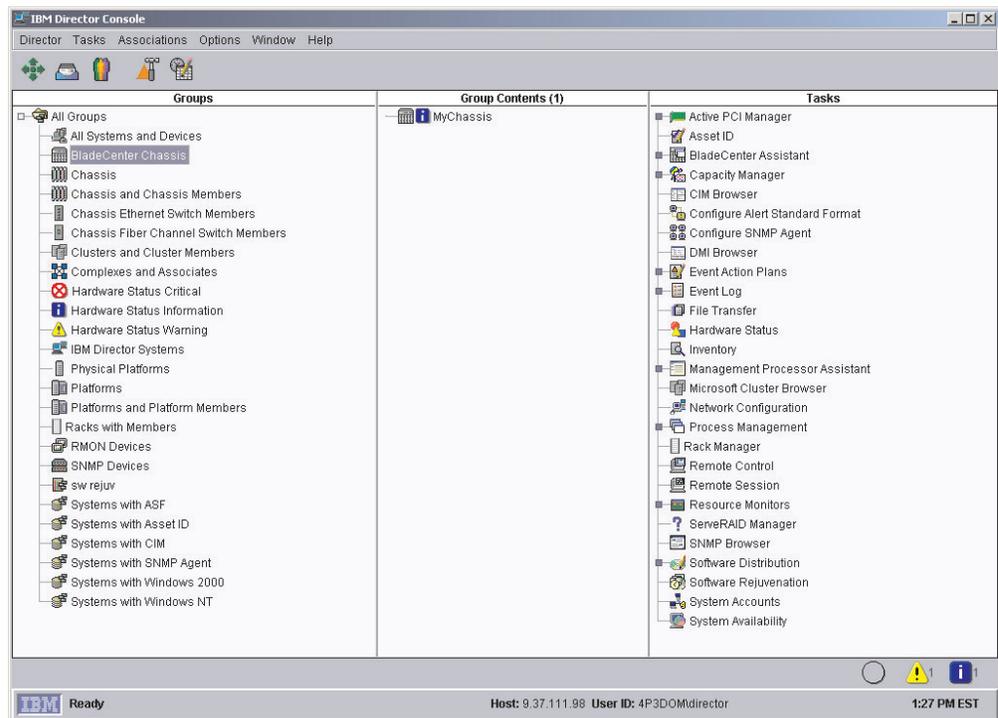


Figure 58. IBM Director Console: Group Contents pane

**Note:** The discovery operation might take several minutes, depending on the number of blade servers, management modules, and switch modules that are installed in the BladeCenter chassis.

## Manually discovering the BladeCenter chassis

If the BladeCenter chassis is on a different subnet than the management server, IBM Director cannot discover the BladeCenter chassis automatically. You must discover the BladeCenter chassis manually.

Complete the following steps to discover the BladeCenter chassis manually:

1. Manually change the IP address of the management module, if it is set to the default IP address. See “Manually changing the IP address of the BladeCenter chassis.” for more information
2. From IBM Director Console, right-click in the Group Contents pane; then click **New → BladeCenter Chassis**. The “Add BladeCenter Chassis” window opens.

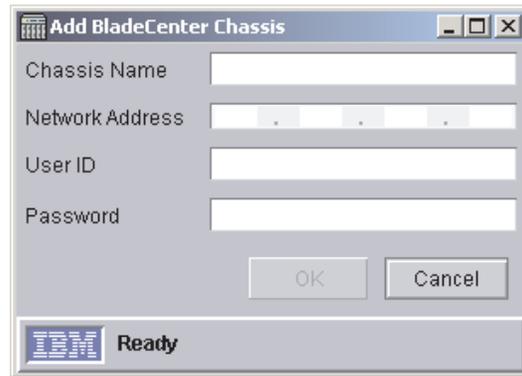


Figure 59. “Add BladeCenter Chassis” window

3. In the **Chassis Name** field, type a name to identify the chassis. This name is displayed in the Groups pane of IBM Director Console.
4. In the **Network Address** field, type the IP address of the external port of the BladeCenter management module.
5. In the **User ID** field, type a valid user ID for the management module.
6. In the **Password** field, type the password that corresponds to the user ID that you typed in step 5.
7. Click **OK**. The BladeCenter chassis managed object is created. It is displayed in the Groups pane of IBM Director Console.

## Manually changing the IP address of the BladeCenter chassis

Complete the following steps to change the IP address of the BladeCenter chassis manually:

1. Using a crossover cable, connect a system to the external port of the management module.
2. Change the IP address of the non-chassis system to an address on the 192.168.70.0 subnet.
3. Using the non-chassis system, open a Web browser.
4. In the **Address** or **Location** field, type the following address and press Enter:  
`http://192.168.70.125`

A password window opens.

5. In the applicable fields, type the default user name (USERID) and password (PASSWORD) for the BladeCenter management module. (Use uppercase letters and a zero, not the letter O.)
6. Click **OK**. The “BladeCenter Management Module” window opens.
7. Click **Continue**. The “System Status Summary” window opens.
8. In the left pane, click **Network Interfaces**. The “Management Module Network Interfaces” window opens.

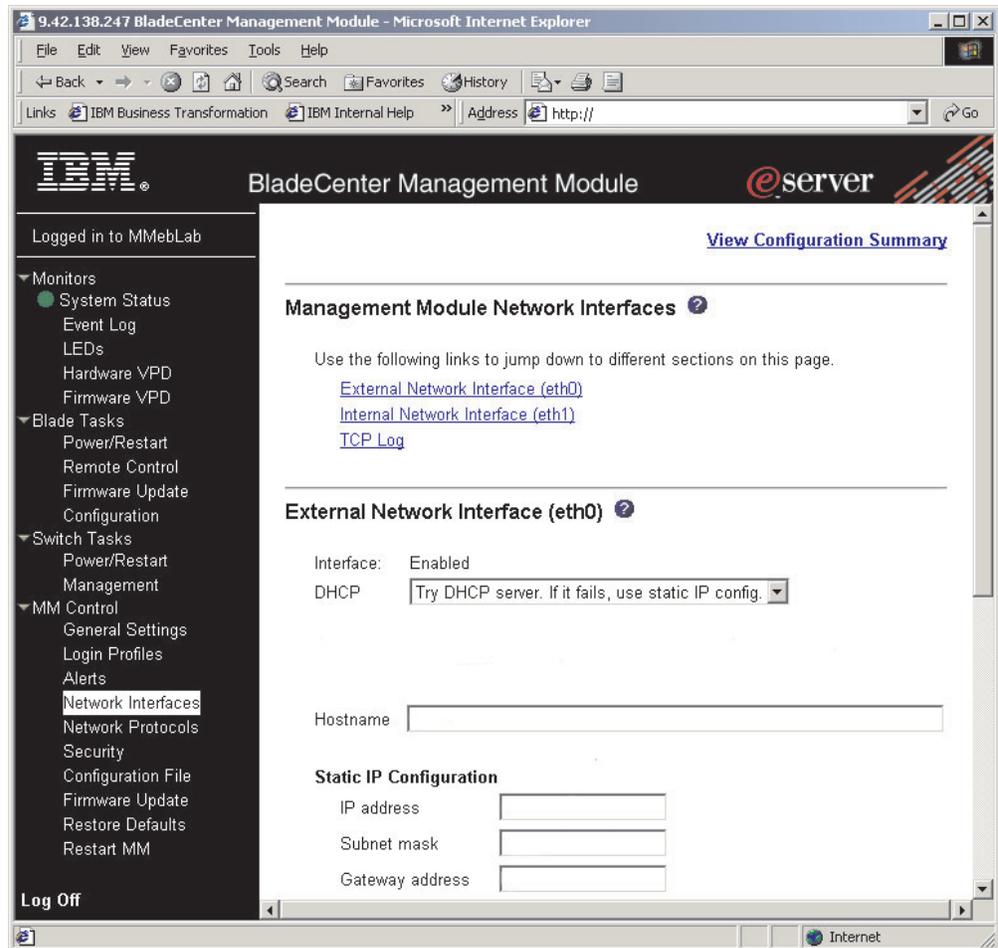


Figure 60. "Management Module Network Interfaces" window

9. In the **DHCP** field, click **Disabled—Use static IP configuration**.
10. In the **IP address** field, type a valid IP address on the same subnet as the management server.
11. In the **Subnet mask** field, type a valid subnet mask.
12. In the **Gateway address** field, type a valid gateway address.
13. Click **Save**.
14. In the left pane, click **Restart MM**.

## Using the BladeCenter Deployment wizard

You can use the BladeCenter Deployment wizard to create a profile that contains BladeCenter chassis configuration information.

You can run the wizard online (targeted against one or more BladeCenter chassis) or offline. When you run the wizard online, you are prompted to configure only those switch modules that are present in the chassis. When you run the wizard offline, you are prompted to configure all the currently supported switch modules. After you run the wizard and create the profile, you can apply it to one or more BladeCenter chassis. If the profile contains configuration information that it is not applicable to a specific BladeCenter chassis, the information is ignored.

You also can use the BladeCenter Deployment wizard to generate an XML file that contains BladeCenter chassis configuration information. You then can use DIRCMD, the IBM Director command-line interface, to create a profile from the XML file. You also can use DIRCMD to apply the profile to one or more BladeCenter chassis. For more information about DIRCMD, see the *IBM Director 4.20 Systems Management Guide*.

## BladeCenter Deployment wizard profiles

You can use the BladeCenter Deployment wizard to create reusable profiles that you can apply to BladeCenter chassis. A profile can contain the following configuration information:

- User names and passwords for the management module and switch modules
- IP addresses for the management module and switch modules
- Network protocol configuration information for the management module and switch modules
- Deployment policies
- Whether or not detect-and-deploy is enabled for the chassis or switch modules

### Chassis detect-and-deploy profiles

You can designate one profile to automatically configure new BladeCenter chassis when they are added to the IBM Director environment. This is the *chassis detect-and-deploy profile*. IBM Director automatically applies the chassis detect-and-deploy profile when it discovers a new BladeCenter chassis or if you create a new BladeCenter chassis managed object.

If you enable a chassis detect-and-deploy policy, be careful when deleting and manually recreating chassis managed objects for previously configured BladeCenter chassis. If you delete and manually recreate a BladeCenter chassis managed object, IBM Director automatically applies the chassis detect-and-deploy profile to that chassis.

### Profiles that include deployment policies

A profile can include deployment policies, if Remote Deployment Manager (RDM) is installed on your management server. A *deployment policy* associates a specific bay in the BladeCenter chassis with an RDM noninteractive task, for example, installing an operating system.

When a profile that includes deployment policies is applied to a BladeCenter chassis, the RDM noninteractive tasks are run on the blade servers in the bays that are assigned deployment policies. The blade servers must be turned off; IBM Director will not shut down or restart (reboot) blade servers that are running.

After you configure a BladeCenter chassis using a profile that contains deployment policies, IBM Director applies the deployment policy whenever a new blade server is inserted in the BladeCenter chassis. IBM Director automatically sets the blade server boot sequence to the local hard disk drive followed by the network. If an operating system is already installed, the blade server starts (boots) from the hard disk drive, and IBM Director does not run the RDM task. However, if the blade server starts (boots) from the network, IBM Director initiates the deployment policy and runs the RDM task.

**Note:** If the BladeCenter chassis contains an IBM HS20 SCSI Storage Expansion unit, IBM Director does not apply the deployment policy when both the following conditions apply:

- The blade server that is used with the storage expansion unit is set to start (boot) from the SCSI hard disk drive.
- You hot-swap the SCSI hard disk drive in the storage expansion unit.

To ensure that the deployment policy is applied to the new SCSI hard disk drive, after hot-swapping the SCSI hard disk drive, remove and reinsert the blade server.

## Creating and applying a BladeCenter Deployment wizard profile

**Note:** You must have a pool of static IP addresses to assign to the management module and switch module configuration ports. To configure one BladeCenter chassis, you must have a minimum of two static IP addresses for the management module and one static IP address for each switch module. The IP addresses must be on the same subnet as the management server.

Complete the following steps to create a BladeCenter Deployment wizard profile:

1. In the IBM Director Console Tasks pane, expand the **BladeCenter Assistant** task.
2. Complete one of the following steps:

<b>If you are running the wizard online</b>	Drag the <b>Deployment Wizard</b> task onto the BladeCenter chassis that you want to configure.
<b>If you are running the wizard offline</b>	Double-click the <b>Deployment Wizard</b> task.

The BladeCenter Deployment wizard starts and the “Welcome to the BladeCenter Deployment wizard” window opens.

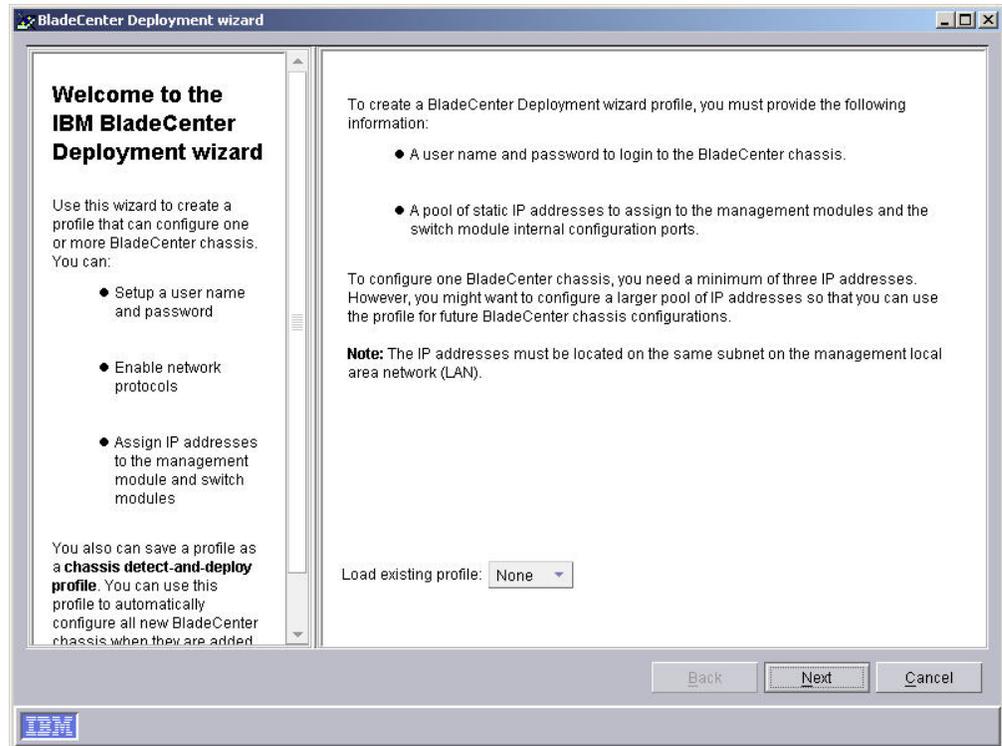


Figure 61. BladeCenter Deployment wizard: “Welcome to the BladeCenter Deployment wizard” window

3. Click **Next**. If you are already logged in to the management module or if you are running the wizard offline, the “Change the user name and password for the management module” window opens. Go to step 6 on page 121. If you are running the wizard against a locked BladeCenter chassis, the “Login to the BladeCenter management module” window opens.

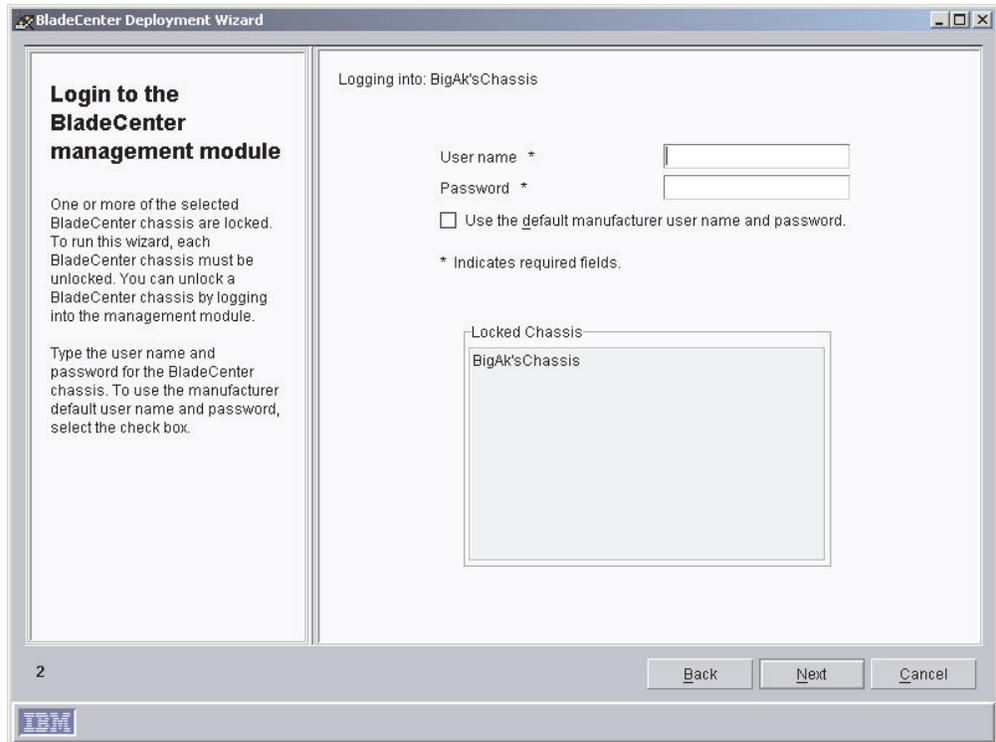


Figure 62. BladeCenter Deployment wizard: “Login to the BladeCenter management module” window

4. Log in to the BladeCenter management module:
  - a. In the **User name** field, type a valid user name for the management module.
  - b. In the **Password** field, type the password that is associated with the user name that you typed in step 4a.To use the default user account and password, select the **Use the factory-default user name and password** check box.
5. Click **Next**. The “Change the user name and password for the management module” window opens.

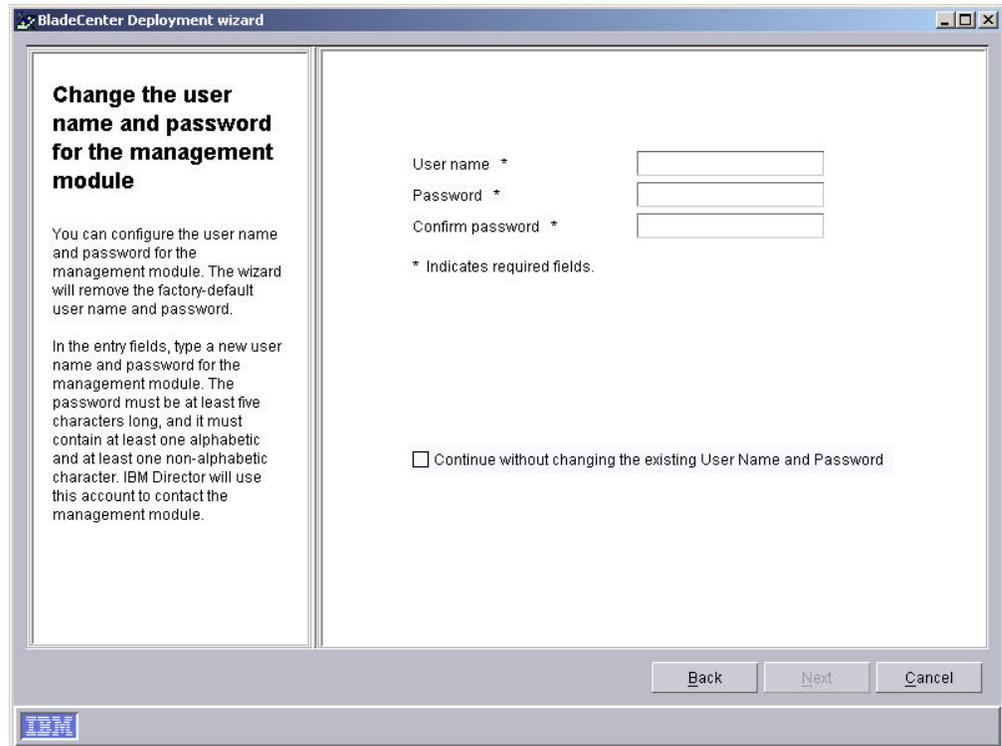


Figure 63. BladeCenter Deployment wizard: “Change the user name and password for the management module” window

6. Configure the user name and password for the BladeCenter chassis:
  - a. In the **User name** field, type a user name.
  - b. In the **Password** and **Confirm password** fields, type a password. It must be at least six characters and contain at least one digit.

If you do not want to change the existing management module user name and password, select the **Continue without changing the existing user name and password** check box.
7. Click **Next**. The “Configure the management module properties” window opens.

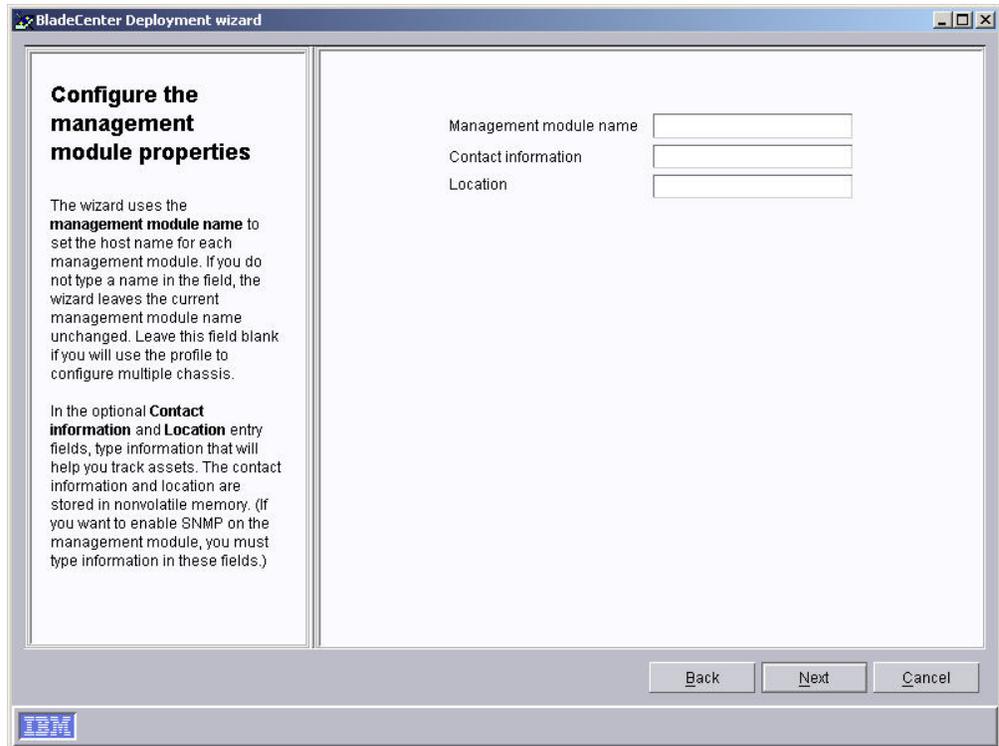


Figure 64. BladeCenter Deployment wizard: “Configure the management module properties” window

8. Configure the management-module properties:
  - a. In the **Management module name** field, type a name for the BladeCenter management module. If you leave this field blank, the BladeCenter management module is assigned the profile name.
  - b. In the **Contact information** field, type the name of the asset owner.
  - c. In the **Location** field, type information about where the BladeCenter is located.

**Note:** If you want to enable SNMP on the management module, you *must* type information in the **Contact information** and **Location** entry fields.
9. Click **Next**. The “Configure the management module protocols” window opens.

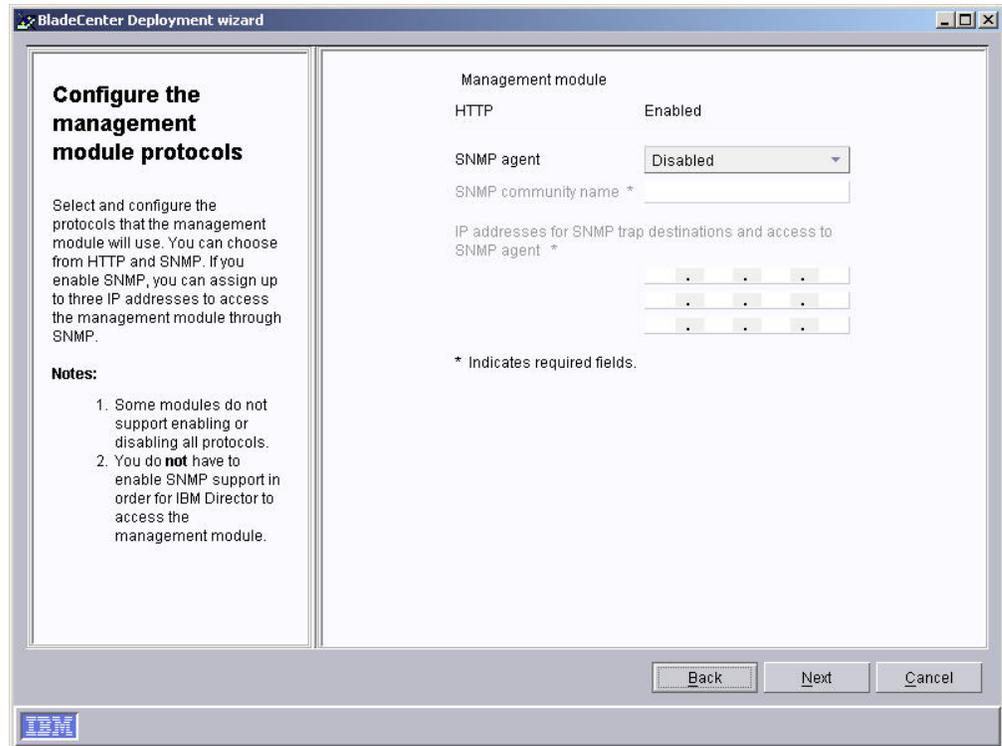


Figure 65. BladeCenter Deployment wizard: “Configure the management module protocols” window

10. Configure the management-module network protocols. HTTP is enabled by default. Complete the following steps to enable SNMP:
  - a. In the **SNMP agent** field, select **Enabled**.
  - b. In the **SNMP community name** field, type a community name. (By default, this is set to public.)
  - c. In the **IP addresses** fields, type at least one and as many as three IP addresses.

**Note:** To enable SNMP on the management module, you *must* have typed information in the **Contact information** and **Location** entry fields in the previous window. To do so now, click **Back** to return to the “Configure the management module properties” window.

11. Click **Next**. The “Configure the IP addresses” window opens.

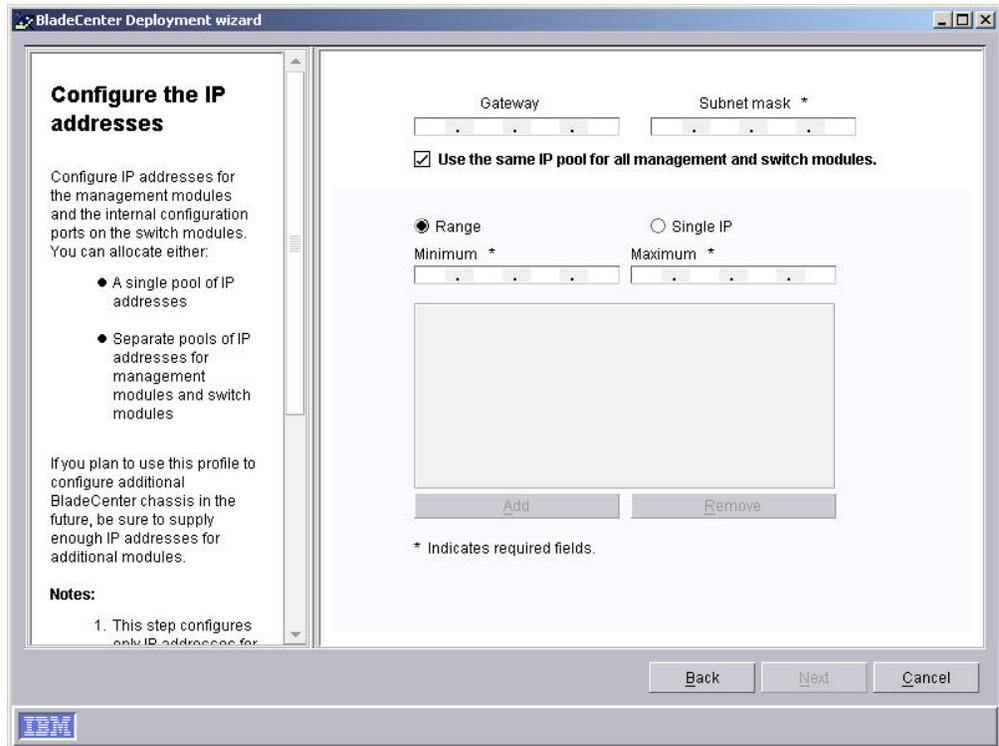


Figure 66. BladeCenter Deployment wizard: “Configure the IP addresses” window

12. Configure the IP settings for the management and switch modules:
  - a. In the **Gateway** field, type the IP address for the network gateway.
  - b. In the **Subnet mask** field, type the IP address for the subnet mask.
13. Assign IP addresses for the management and switch modules:
  - a. To use one pool of IP addresses for both the management and switch modules, create a pool of IP addresses. You can add IP addresses to the pool individually or by specifying a range:
    - To add a single IP address to the pool, click **Single IP**. In the **IP address** field, type the IP address; then, click **Add**.
    - To add a range of IP addresses, click **Range**. In the **Minimum** and **Maximum** fields, type the IP addresses that specify the range. Click **Add**.
  - b. To assign separate pools of IP addresses to the management and switch modules, clear the **Use the same IP pool for all management and switch modules** check box. The **Management module** and **Switch module** tabs are displayed.
    - To create the pool of IP addresses for the management modules, click **Management module** and follow the instructions in step 13a.
    - To create the pool of IP addresses for the switch modules, click **Switch module** and follow the instructions in step 13a.
14. Click **Next**. The “Change the user name and password for the switch modules” window opens.

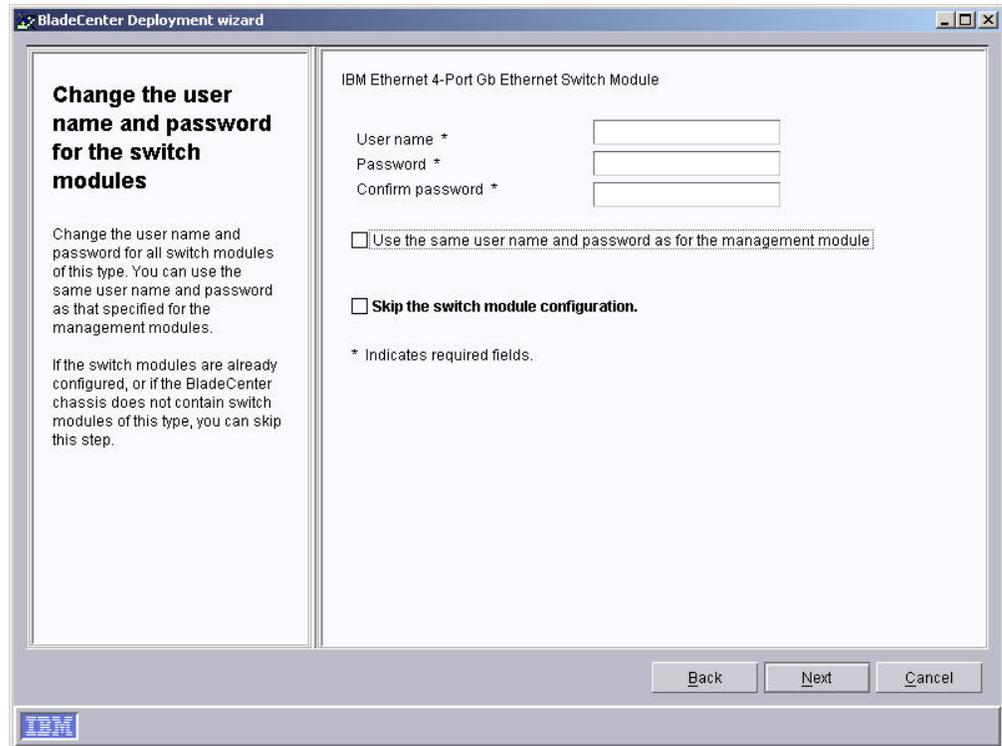


Figure 67. BladeCenter Deployment wizard: “Change the user name and password for the switch modules” window

15. Configure the user name and password for this type of switch module. Take one of the following actions:
  - a. To use the same information for both the management module and the switch module, select the **Use the same user name and password as for the management module** check box. (This option is not available if a user name and password for the management module has not been specified.)
  - b. To assign a new user name and password to the switch module, in the applicable fields, type a new user name and password.
  - c. If the switch modules are configured already or you do not want to configure this type of switch module, select the **Skip the module configuration** check box. Go to step 18 on page 127.
16. Click **Next**. The “Configure the switch module” window opens.

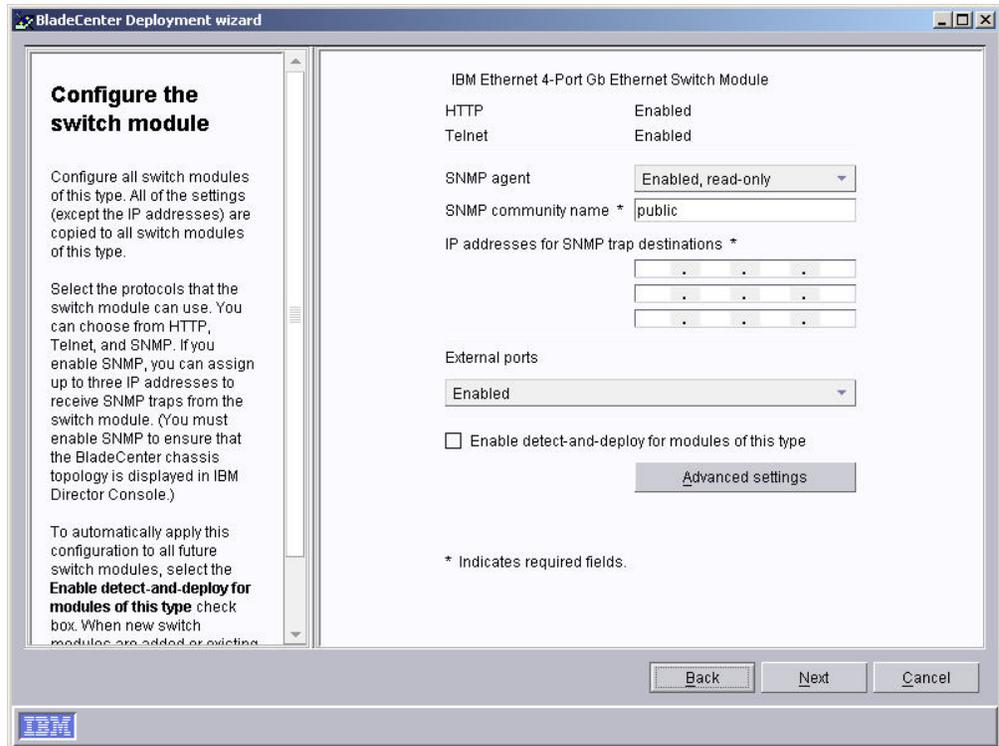


Figure 68. BladeCenter Deployment wizard: “Configure the switch module” window

17. Configure the network protocols for this type of switch module:
  - a. To enable HTTP, in the **HTTP** field, select **Enabled**. (This option is not available for all switch modules.)
  - b. To enable Telnet, in the **Telnet** field, select **Enabled**. (This option is not available for all switch modules.)
  - c. To enable SNMP, in the **SNMP agent** field, select **Enabled** or **Enabled, read-only**. Then, complete the following tasks:
    - 1) In the **SNMP community name** field, type a community name. By default, this is set to `public`.
    - 2) In the **IP addresses** fields, type at least one and as many as three IP addresses. These addresses receive SNMP traps from the switch module.

**Note:** You must enable SNMP if you want the switch module to appear in the BladeCenter chassis topology that is displayed in IBM Director Console.
  - d. To enable the external ports of the switch modules, select **Enabled**. If you are configuring an IBM Ethernet 4-Port Gb Ethernet Switch Module, you also can configure the external ports as link aggregation groups (trunks). Before you do so, make sure that the LAN switch has a compatible multiport trunk configuration.

- e. To automatically apply this configuration to all switch modules of this type, select the **Enable detect-and-deploy for modules of this type** check box. When switch modules of this type are inserted in the BladeCenter chassis, this configuration is applied automatically.
- f. Click **Advanced settings** to perform one of the following tasks:
- g.

<b>If you are running the wizard online</b>	Start the switch vendor software and configure additional settings.
<b>If you are running the wizard offline</b>	Load a configuration file. You can create a configuration file by using the vendor software to back up the switch module configuration.

18. Take one of the following actions:
  - If you are running the wizard online and have not yet configured all the switch modules in the BladeCenter chassis, repeat step 14.
  - If you are running the wizard online and have configured all the switch modules in the BladeCenter chassis, go to step 19.
  - If you are running the wizard offline, repeat steps 14-17 until you have configured each of the supported types of switch modules.
  - If you are running the wizard offline and have configured all of the switch modules, go to step 19.
19. Click **Next**. The “Deploy the operating systems to the blade servers” window opens.

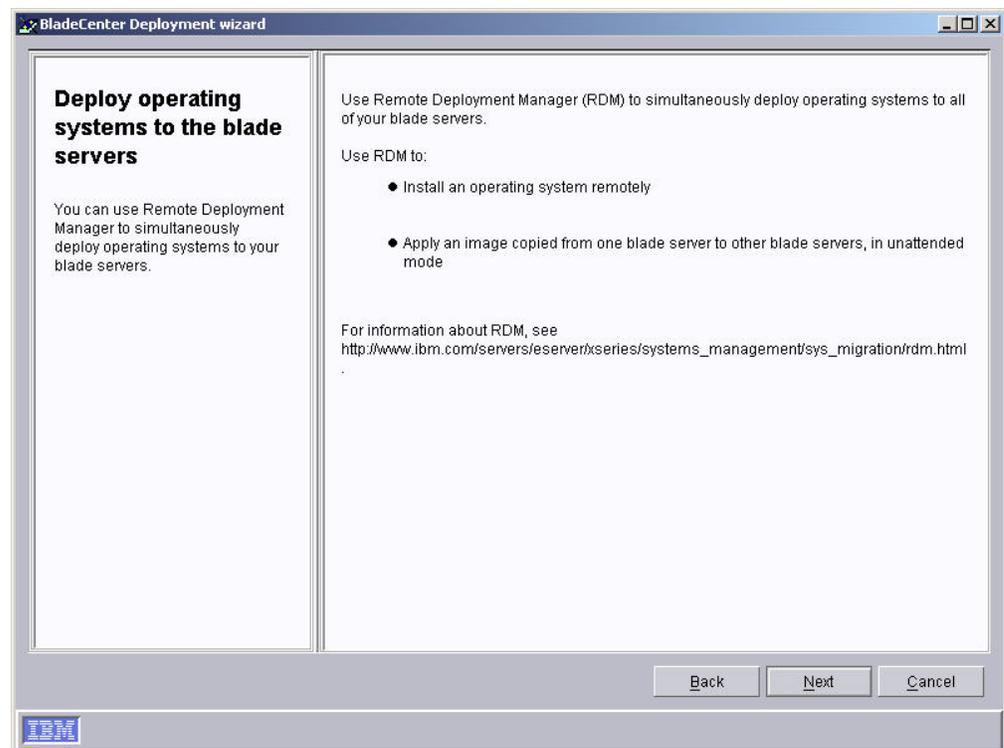


Figure 69. BladeCenter Deployment wizard: “Deploy operating systems to the blade servers” window

20. If Remote Deployment Manager (RDM) is installed on your management server, go to step 21. Otherwise, go to step 24.
21. Click **Next**. The “Configure the deployment policies” window opens.

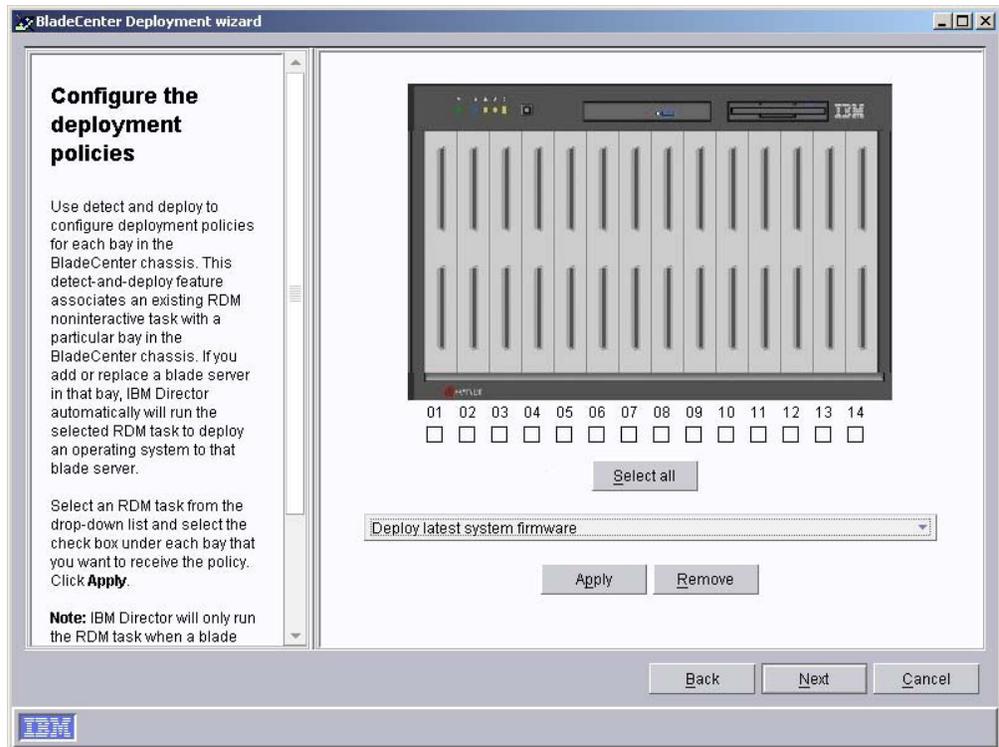


Figure 70. BladeCenter Deployment wizard: “Configure the deployment policies” window

22. Select an RDM task from the drop-down list and select the check box under each bay that you want to receive the policy. Click **Apply**.
23. Repeat step 22 until you have configured all the deployment policies.
24. Click **Next**. The “Setup summary” window opens.

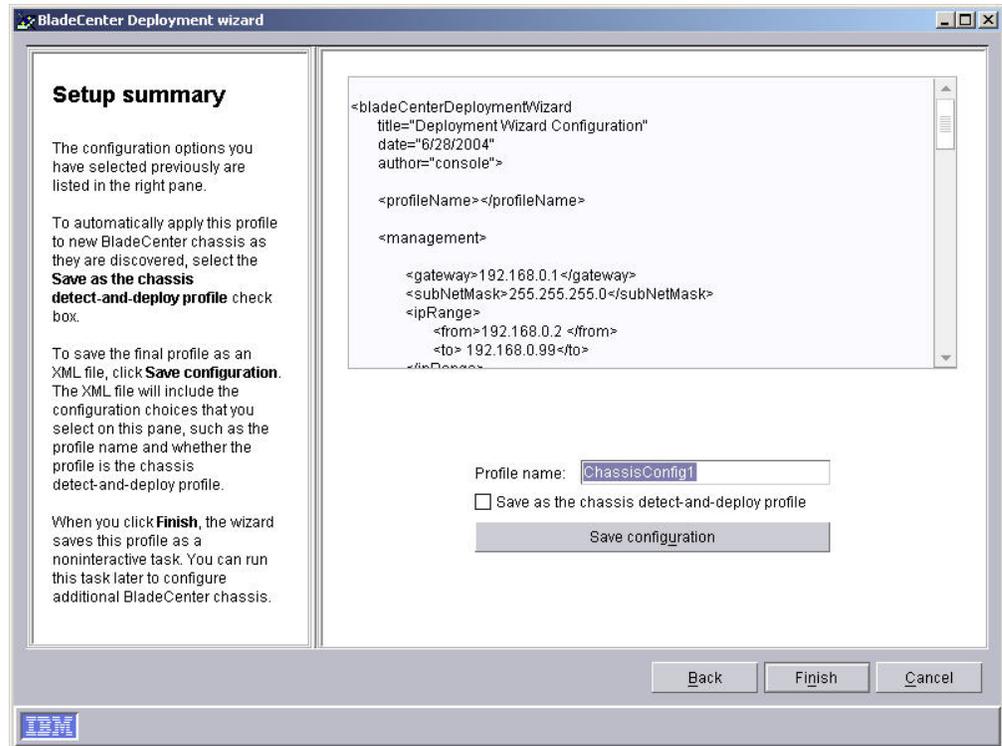


Figure 71. BladeCenter Deployment wizard: “Setup summary” window

25. Review the profile configuration, which is displayed as an XML file in the right pane. The XML file contains all the previously-selected options, but it does not contain the options that you select on this window: profile name and whether the profile is designated as the chassis detect-and-deploy profile.

Complete configuring the profile:

- a. In the **Profile name** field, type a name for the profile. By default, the profile is given the name that you assigned to the management module. When you run the profile against a BladeCenter chassis, the chassis managed object is assigned the profile name.
- b. To apply this profile automatically to all new BladeCenter chassis when they are discovered by IBM Director, select the **Save as the chassis detect-and-deploy profile** check box.

**Attention:** There can be only one chassis detect-and-deploy profile. If a chassis detect-and-deploy profile already exists and you select the **Save as the chassis detect-and-deploy profile** check box, you will overwrite the existing profile.

- c. To save the profile configuration as an XML file, click **Save configuration**. You can edit the XML file and then use DIRCMD, the IBM Director command-line interface, to create the BladeCenter Deployment wizard profile.
26. Click **Finish**. The profile is created. It appears as a subtask under Deployment Wizard in the Tasks pane of IBM Director Console.

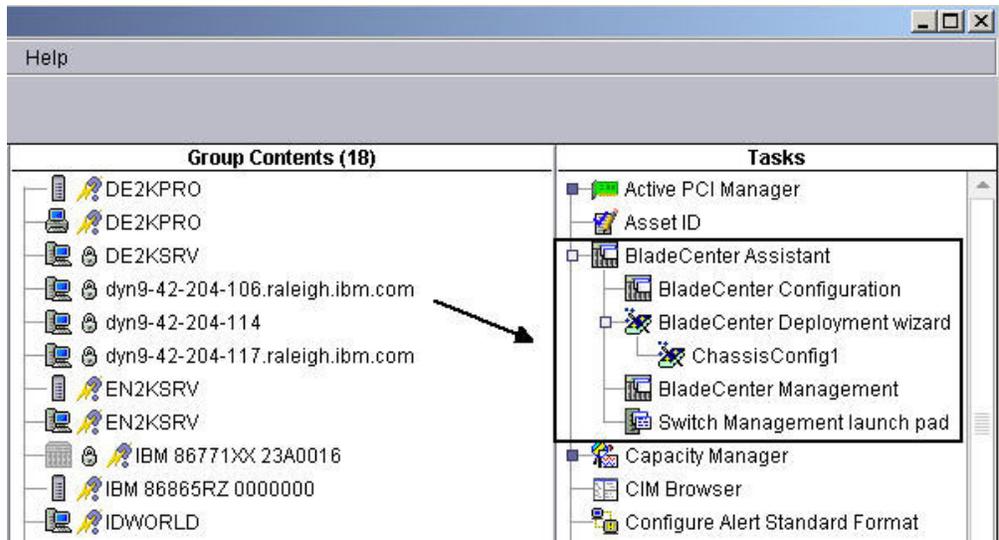


Figure 72. IBM Director Console Tasks pane: BladeCenter Deployment wizard profile

27. To apply the profile, complete one of the following actions:

---

**If you are running the wizard online** When prompted, select when you want to run the profile. You can select to run the profile now, schedule a task, or cancel.

---

**If you are running the wizard offline** Drag the profile onto the BladeCenter chassis that you want to configure. You can select to run the profile now, schedule a task, or cancel.

---

---

## Chapter 9. Installing IBM Director extensions

This chapter contains procedures for the following tasks:

- Completing the Rack Manager installation on the management server
- Installing IBM Director Software Distribution (Premium Edition) on the management server
- Installing the IBM Director Server Plus extensions on managed systems

The IBM Server Plus Pack extensions are installed on the management server during the installation of IBM Director Server. For more information, see Chapter 4, “Installing IBM Director Server,” on page 39.

---

### Completing the Rack Manager installation on the management server

**Note:** If you did not install Rack Manager when you installed IBM Director Server, do so before continuing with this procedure. For information about modifying an IBM Director Server installation to add Rack Manager, see “Modifying an IBM Director installation” on page 197.

To complete the Rack Management installation on the management server, you must install the Rack Management component which is on the *IBM Director Server Plus Pack* CD. This section contains procedures for installing this component on management servers running either Linux or Windows.

### Completing the Rack Manager installation on Linux

Complete the following steps to finish installing Rack Manager on a management server running Linux:

1. Stop IBM Director. From a command prompt, type the following command and press Enter:

```
/opt/IBM/director/bin/twgstop
```

2. Insert the *IBM Director Server Plus Pack* CD into the CD-ROM drive.
3. If the CD does not automount, go to step 4. If the CD automounts, type the following command and press Enter:

```
umount /mnt/cdrom
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

4. Type the following command and press Enter:

```
mount -t iso9660 -o map=off /dev/cdrom /mnt/cdrom
```

where *dev/cdrom* is the specific device file for the CD-ROM block device and *mnt/cdrom* is mount point of the CD-ROM drive.

5. Change to the directory where the installation script is located. Type the following command and press Enter:

```
cd /mnt/cdrom/rackmgr/server/linux/i386/
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

6. Type the following command and press Enter:

```
./install
```

7. To start IBM Director, type the following command and press Enter:

```
/opt/IBM/director/bin/twgstart
```

8. To unmount the CD-ROM drive, complete the following steps:
  - a. Type `cd /` and press Enter.
  - b. Type the following command and press Enter:

```
umount /mnt/cdrom
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

9. Remove the *IBM Director Server Plus Pack* CD from the CD-ROM drive.

## Completing the Rack Manager installation on Windows

Complete the following steps to finish installing Rack Manager on a management server running Windows:

1. Insert the *IBM Director Server Plus Pack* CD into the CD-ROM drive.
2. Start Windows Explorer, and open the `\rackmgr\server\windows\i386` directory, which is on the *IBM Director Server Plus Pack* CD.
3. Double-click **setup.exe**. The InstallShield wizard starts, and the “Welcome to the InstallShield Wizard” window opens.
4. Click **Next**. A window that contains the license agreement opens.
5. Click **Yes** to accept the license agreement. The “Start Copying Files” window opens.
6. Click **Next**. The “InstallShield Wizard Complete” window opens.
7. Click **Finish**.
8. Remove the *IBM Director Server Plus Pack* CD from the CD-ROM drive.
9. Shut down and restart the management server.

---

## Installing Software Distribution (Premium Edition)

You can install Software Distribution (Premium Edition) on management servers running i5/OS, Linux, and Windows.

## Installing Software Distribution on i5/OS

Complete the following steps to install Software Distribution on the management server:

1. Locate a server with a CD-ROM drive that you can use to copy files to management server.
2. Insert the *IBM Director Software Distribution (Premium Edition)* CD into the CD-ROM drive.
3. Change to the `/swdist/server/os400` directory.
4. Copy the contents of the `/swdist/server/os400` directory to the `/qibm/proddata/director/bin/` directory on the management server.
5. Remove the *IBM Director Software Distribution (Premium Edition)* CD from the CD-ROM drive.
6. From a command prompt on the management server, type the following command and press Enter:

```
cd /qibm/proddata/director/bin
```
7. Type the following command and press Enter:

```
install
```
8. Shut down and restart the management server.

## Installing Software Distribution on Linux

Complete the following steps to install Software Distribution on the management server:

1. Stop IBM Director. From a command prompt, type the following command and press Enter:

```
/opt/IBM/director/bin/twgstop
```

2. Insert the *IBM Director Software Distribution (Premium Edition)* CD into the CD-ROM drive.
3. If the CD does not automount, go to step 4. If the CD automounts, type the following command and press Enter:

```
umount /mnt/cdrom
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

4. Type the following command and press Enter:

```
mount -t iso9660 -o map=off /dev/cdrom /mnt/cdrom
```

where *dev/cdrom* is the specific device file for the CD-ROM block device and *mnt/cdrom* is mount point of the CD-ROM drive.

5. Change to the directory where the installation script is located. Type the following command and press Enter:

```
cd /mnt/cdrom/swdist/server/linux/i386/
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

6. Type the following command and press Enter:

```
./install
```

7. To start IBM Director, type the following command and press Enter:

```
/opt/IBM/director/bin/twgstart
```

8. To unmount the CD-ROM drive, complete the following steps:

- a. Type `cd /` and press Enter.

- b. Type the following command and press Enter:

```
umount /mnt/cdrom
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

9. Remove the CD from the CD-ROM drive.

## Installing Software Distribution on Windows

Complete the following steps to install Software Distribution on the management server:

1. Insert the *IBM Director Software Distribution (Premium Edition)* CD into the CD-ROM drive.
2. Start Windows Explorer, and open the `\swdist\server\windows\i386` directory, which is on the *IBM Director Software Distribution (Premium Edition)* CD.
3. Double-click **setup.exe**. The InstallShield wizard starts and the “Welcome to the InstallShield Wizard” window opens.
4. Click **Next**. A window that contains the license agreement opens.
5. Click **Yes** to accept the license agreement. The “Start Copying Files” window opens.
6. Click **Next**. The “InstallShield Wizard Complete” window opens.
7. Click **Finish**.

8. Remove the *IBM Director Software Distribution (Premium Edition)* CD from the CD-ROM drive.
9. Shut down and restart the management server.

---

## Preparing to install the Server Plus Pack extensions on managed systems

If you plan to run Active PCI Manager against a managed system, make sure that IBM Active PCI Software and any other requisite code is installed on the managed system. The following table contains information about the software that is a prerequisite for running Active PCI Manager.

*Table 20. IBM Active PCI Software necessary to run Active PCI Manager*

Operating system	Requisite
Windows	<ul style="list-style-type: none"> <li>• IBM Active PCI Software for Microsoft Windows, version 5.1.1.1 or later, must be installed.</li> </ul>
SUSE LINUX Enterprise Server 8	<ul style="list-style-type: none"> <li>• IBM Active PCI Software for SUSE LINUX Enterprise Server 8, version 1.0 or later, must be installed.</li> <li>• Advanced Configuration and Power Interface (ACPI) code must be enabled.</li> </ul>

You can download the IBM Active PCI software from <http://www.ibm.com/support/>. In the **Search** field in the upper-right corner of the page, type `activepci`.

To run the Fault Tolerant Management Interface (a subtask of Active PCI Manager) against a managed system, the managed system must have the applicable device driver installed. The following table lists the minimum version of the supported device drivers for each network adapter.

*Table 21. Network adapter device drivers necessary to run the Fault Tolerant Management Interface*

Manufacturer	Version
Intel	8.3
3Com	2.3
Broadcom	6.85

Make sure that the applicable device driver is installed and that the device driver is at the supported version or later.

---

## Installing the Server Plus Pack extensions on managed systems

The *IBM Director Server Plus Pack* CD contains the Server Plus Pack extensions. You can install them on managed systems either by using standard installation procedures or by using the IBM Director Software Distribution task.

For a list of Server Plus Pack extensions that can be installed on managed systems and the operating systems on which they are supported, see “Server Plus Pack extensions” on page 17.

## Using standard installation procedures

You can use standard installation procedures to install the Server Plus Pack extensions on managed systems. This is useful for managed systems running operating systems that do not support software distribution, such as Novell NetWare.

### Installing the Server Plus Pack extensions on Linux

Complete the following steps to install the Server Plus Pack extensions on a managed system running Linux:

1. Stop IBM Director Agent. From a command prompt, type the following command and press Enter:
2. Insert the *IBM Director Server Plus Pack* CD into the CD-ROM drive.
3. If the CD does not automount, go to step 4. If the CD automounts, type the following command and press Enter:

```
/opt/IBM/director/bin/twgstop
```

```
umount /mnt/cdrom
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

4. Type the following command and press Enter:

```
mount -t iso9660 -o map=off /dev/cdrom /mnt/cdrom
```

where *dev/cdrom* is the specific device file for the CD-ROM block device and *mnt/cdrom* is mount point of the CD-ROM drive.

5. Change to the directory where the RPM files are located. Type one of the following commands and press Enter:

<b>For Active PCI Manager</b>	<code>cd /mnt/cdrom/activpci/agent/linux/i386/sles_8</code>
<b>For Capacity Manager</b>	<code>cd /mnt/cdrom/capmgt/agent/linux/i386/</code>
<b>For Software Rejuvenation</b>	<code>cd /mnt/cdrom/swrejuv/agent/linux/i386/</code>
<b>For System Availability</b>	<code>cd /mnt/cdrom/sysavail/agent/linux/i386/</code>

where *mnt/cdrom* is the mount point of the CD-ROM drive.

6. Install the Server Plus Pack extension. Type one of the following commands and press Enter:

<b>For Active PCI Manager</b>	<code>rpm -U ActivePCIManagerAgent-4.20-1.i386.rpm</code>
<b>For Capacity Manager</b>	<code>rpm -U CapMgtAgent-4.20-1.i386.rpm</code>
<b>For Software Rejuvenation</b>	<code>rpm -U SwRejuvAgent-4.20-1.i386.rpm</code>
<b>For System Availability</b>	<code>rpm -U SysAvailAgent-4.20-1.i386.rpm</code>

7. Repeat steps 5 and 6 until you have installed all the Service Plus Pack extensions that you want to install.
8. To start IBM Director Agent, type the following command and press Enter:

```
/opt/IBM/director/bin/twgstart
```

9. To unmount the CD-ROM drive, complete the following steps:
  - a. Type `cd /` and press Enter.
  - b. Type the following command and press Enter:

```
umount /mnt/cdrom
```

where `mnt/cdrom` is the mount point of the CD-ROM drive.

10. Remove the *IBM Director Server Plus Pack* CD from the CD-ROM drive.

## Installing the Server Plus Pack extensions on NetWare

### Notes:

1. To install Capacity Manager, you must log on to the server running NetWare from a Windows workstation running the NetWare Client for Windows.
2. The SYS volume must be mapped as a drive to the system running Windows.
3. You must have administrator or supervisor access on the NetWare server.

Complete the following steps to install Capacity Manager on NetWare:

1. Stop IBM Director Agent. From the server running NetWare, change to the console screen. Type the following command and press Enter:

```
unload twgipc
```
2. Insert the *IBM Director Server Plus Pack* CD into the CD-ROM drive of the system running Windows.
3. Start Windows Explorer and open the `\capmgt\agent\netware` directory.
4. Double-click **setup.exe**. The InstallShield wizard starts, and the “Welcome to the InstallShield Wizard” window opens.
5. Click **Next**. The “Choose Destination Location” window opens.

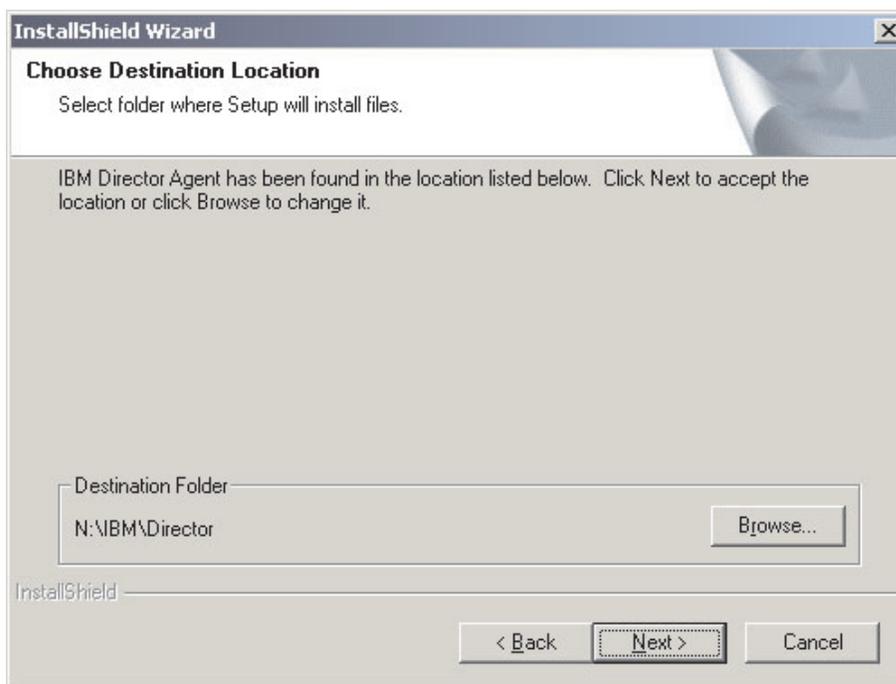


Figure 73. Installing Capacity Manager on NetWare: “Choose Destination Location” window

6. Click **Next**. The “Start Copying Files” window opens.

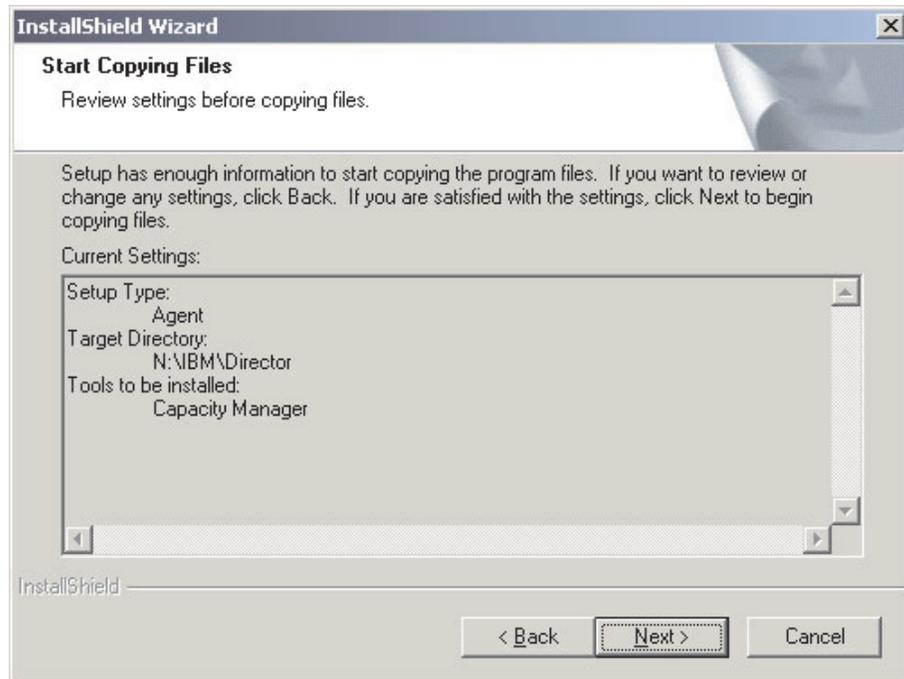


Figure 74. Installing Capacity Manager on NetWare: “Start Copying Files” window

7. Click **Next**. When the installation is completed, the “InstallShield Wizard Complete” window opens.
8. Click **Finish**.
9. Remove the *IBM Director Server Plus Pack* CD from the CD-ROM drive.
10. On the server running NetWare, change to the console screen.
11. To start IBM Director Agent, type the following command and press Enter:
 

```
load twgipc
```

### Installing the Server Plus Pack extensions on Windows

Complete the following steps to install Server Plus Pack extensions on a managed system running Windows:

1. Insert the *IBM Director Server Plus Pack* CD into the CD-ROM drive.
2. Using Windows Explorer, locate the setup.exe file for the Server Plus Pack extension that you want to install. This file is on the *IBM Director Server Plus Pack* CD in the `\extension\agent\windows\i386` directory, where *extension* is one of the following strings:
  - activpci
  - capmgt
  - swrejuv
  - sysavail
3. Double-click the setup.exe file. The IBM Director installation program starts.
4. Follow the instructions on the screen.

## Using the IBM Director Software Distribution task (Windows and Linux only)

The *IBM Director Server Plus Pack* CD contains XML files that describe the Server Plus Pack extensions. The following files are in the root directory of the CD:

- pluspack\_all.xml
- pluspack\_linux.xml
- pluspack\_windows.xml

Each XML file describes a group of a software packages. For example, the pluspack\_all.xml file describes *all* the Server Plus Pack software packages, and the pluspack\_linux.xml file describes the Server Plus Pack packages for managed systems running Linux.

When you import the XML files into the IBM Director, the Director Update Assistant creates software packages. Then, you can use the IBM Director Software Distribution task to distribute the packages to the managed systems.

The names of the non-English-language XML files are similar to those that are listed, with the addition of language codes. For example, the package that describes all the German-language Server Plus Pack software packages is named pluspack\_all\_de.xml.

In addition, XML files that describe the individual Server Plus Pack extensions are in the applicable directories on the *IBM Director Server Plus Pack* CD.

### Creating a software package

You can create software packages that contain the entire Server Plus Pack, packages that contain a single component, or packages that contain several Server Plus Pack components. Complete the following steps to create a software package:

1. Start IBM Director Console.
2. In the Tasks pane, double-click **Software Distribution**. The “Software Distribution Manager” window opens.



Figure 75. Creating a software package: “Software Distribution Manager” window (Standard Edition)



Figure 76. Creating a software package: “Software Distribution Manager” window (Premium Edition)

3. If you have not installed IBM Director 4.20 Software Distribution (Premium Edition), go to step 4. Otherwise, expand the **Wizards** tree.
4. Double-click **Director Update Assistant**. The “Director Update Assistant” window opens.

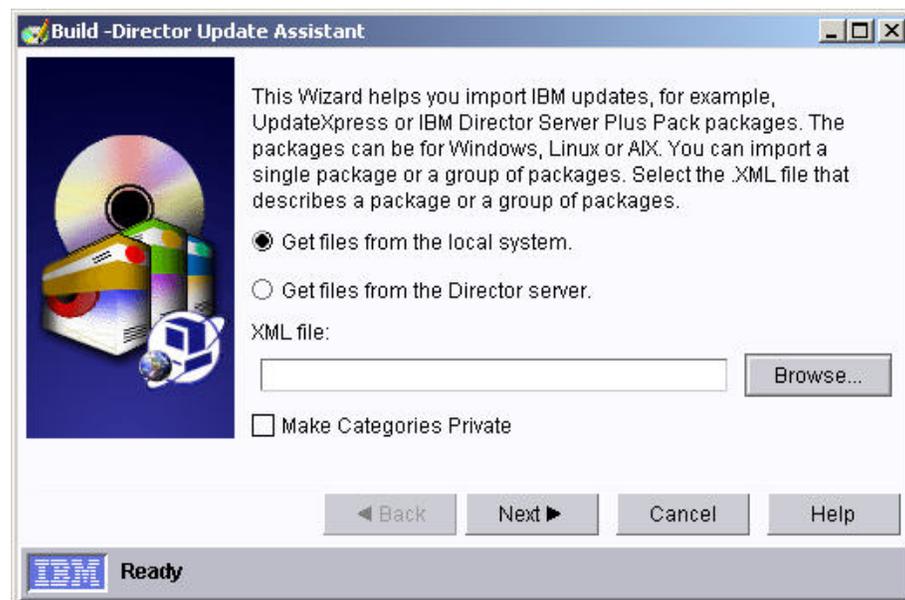


Figure 77. Creating a software package: “Director Update Assistant” window

5. By default, **Get files from the local system** is selected. If you want to get files from the management server, click **Get files from the Director server**.
6. To select a file, click **Browse**. The “IBM Update Package/Root Directory Location” window opens.

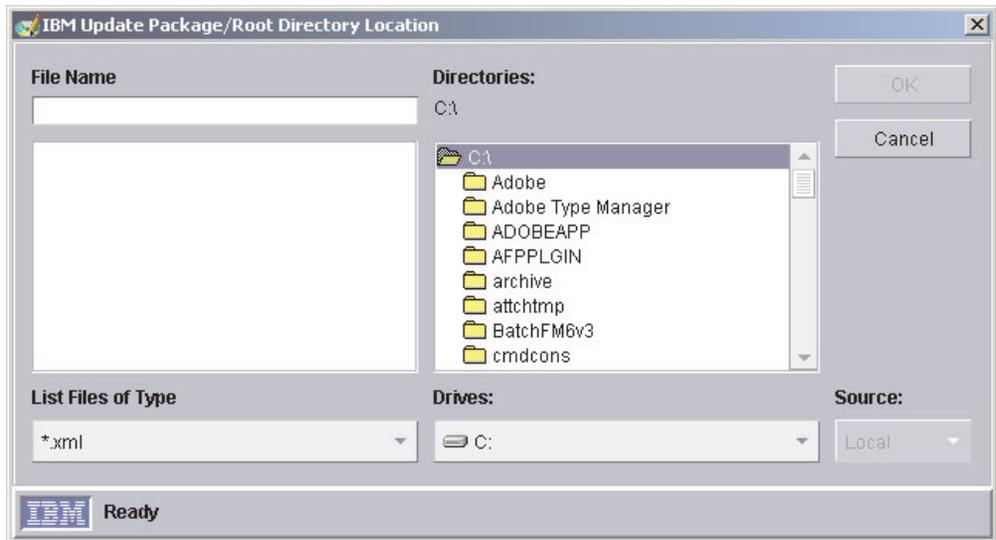


Figure 78. Creating a software package: “IBM Update Package/Root Directory Location” window

7. Locate the XML file and click it. The name of the XML file is displayed in the **File Name** field.

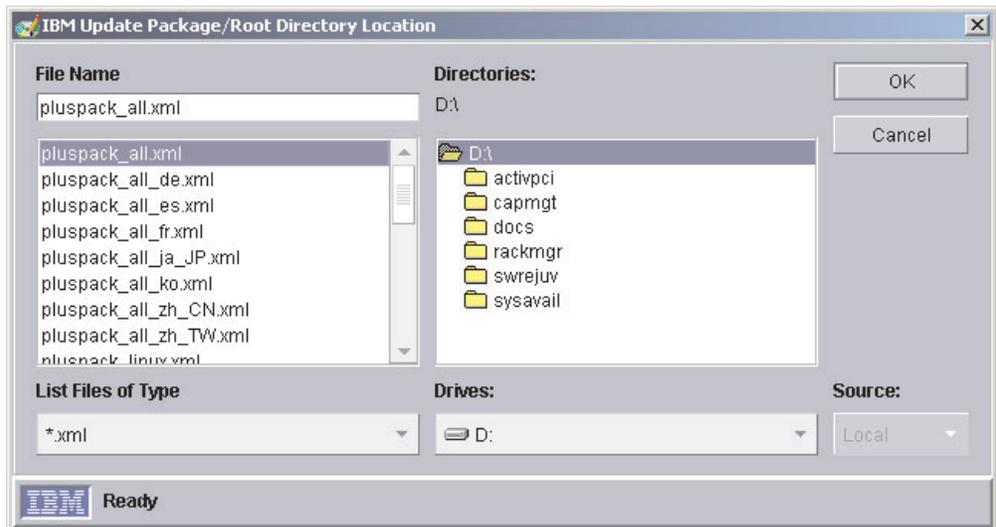


Figure 79. Creating a software package: “IBM Update Package/Root Directory Location” window

8. Click **OK**. The “Director Update Assistant” window reopens. The name of the XML file is displayed in the **XML file** field.
9. Click **Next**. The second “Director Update Assistant” window opens.

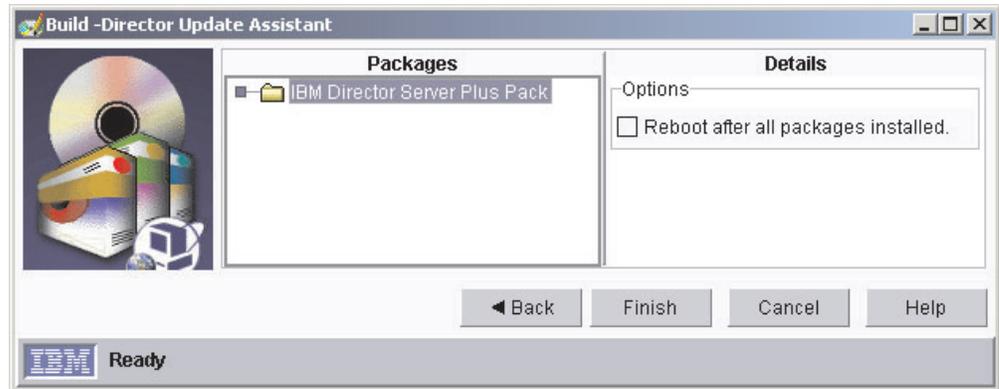


Figure 80. Creating software packages: “Director Update Assistant” window

10. If you selected an XML file that contains more than one update, expand the tree in the Packages pane. A green check mark (✓) is displayed beside the packages that are selected for installation; a red X is displayed beside the update packages that are not selected. To select an update package, double-click the package name.

It is not necessary to select the **Reboot after all packages installed** check box. Installing the Server Plus Pack extension forces a restart of IBM Director Agent, if needed.

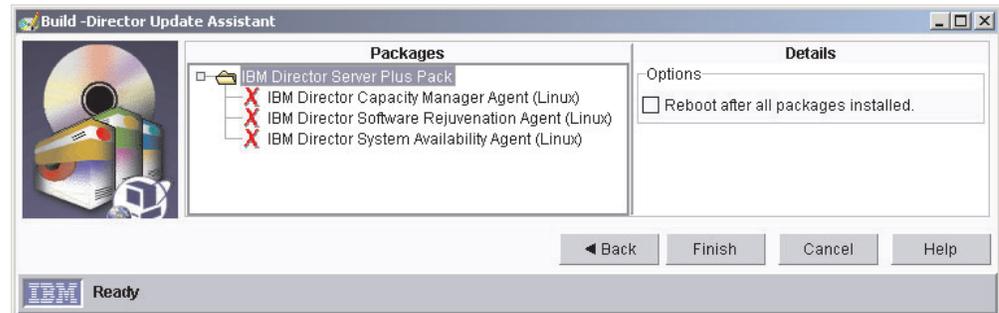


Figure 81. Creating software packages: “Director Update Assistant” window

11. Click **Finish**. As the packages are processed, a status message is displayed at the bottom of the window. When the processing is completed, the software packages are displayed in the Tasks pane of IBM Director Console.

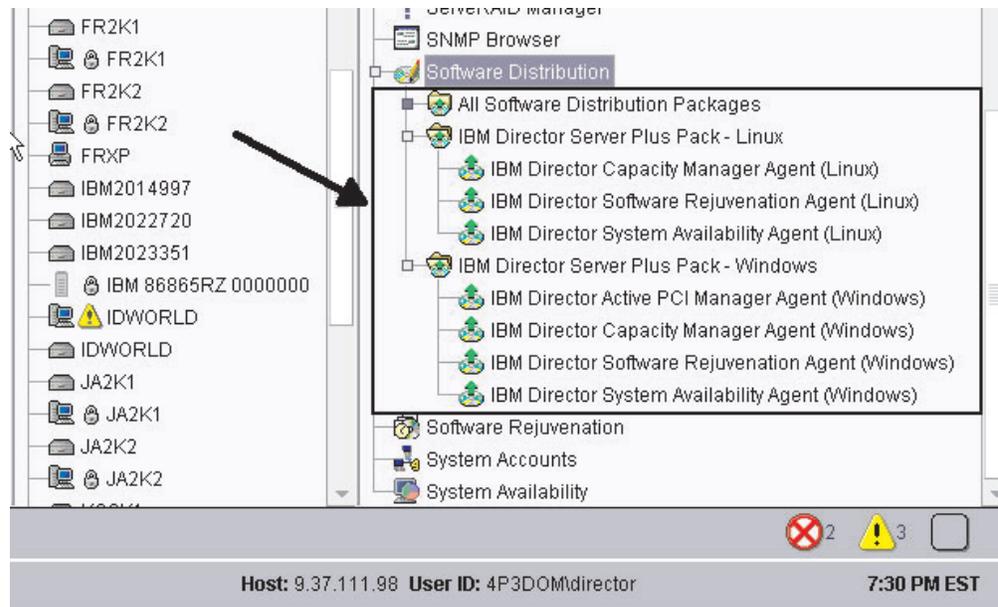


Figure 82. All Software Distribution Packages: IBM Director Server Plus Pack

## Installing a software package

Complete the following steps to install a software package:

1. Start IBM Director Console.
2. In the Tasks pane, expand the **Software Distribution** task.
3. Click the software package or package category that you want to distribute. Then, drag it into the Group Contents pane and drop it onto the icon that is displayed for the system on which you want to install the software package. A window opens.

**Note:** To distribute software to several systems at once, you can drag the software package into the Groups pane and drop it onto the icon for the group. Alternatively, you can select multiple managed systems in the Group Contents pane.

4. When prompted Do you wish to create a scheduled job for this task or execute immediately?, click **Schedule** or **Execute Now**. If you click **Execute Now**, the software package is distributed immediately. If you click **Schedule**, the “New Scheduled Job” window opens.

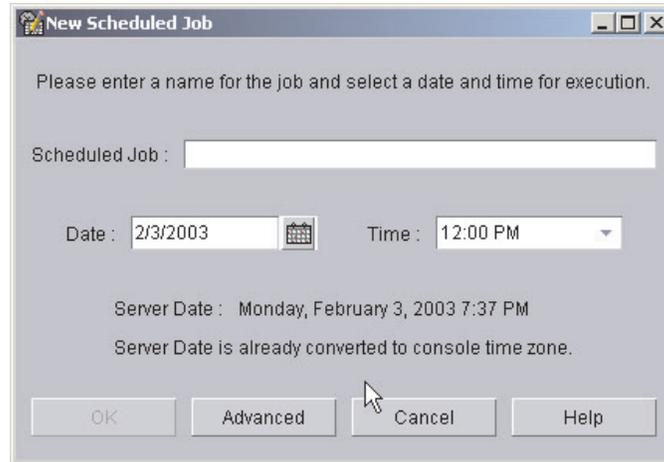


Figure 83. Scheduling the installation of a software package: “New Scheduled Job” window

5. Schedule the job:

- a. In the **Scheduled Job** field, type a unique name for the job. This name is displayed in the Jobs pane of the Scheduler window.
- b. In the **Date** field, type the day you want the software package to be installed (MM/DD/YYYY format).
- c. In the **Time** field, type the time you want the software package to be installed.

For more information about the Scheduler task, see the *IBM Director 4.20 Systems Management Guide*.

6. Click **OK**. The “Save Job Confirmation” window opens.
7. Click **OK**.

After installing Active PCI Manager, be sure to restart (reboot) the managed system. If you do not restart the managed system, the Slot Manager subtask might fail.



---

## Part 4. Upgrading IBM Director



---

## Chapter 10. Upgrading IBM Director Server

This chapter contains instructions for upgrading IBM Director Server.

You can upgrade to IBM Director Server 4.20 from IBM Director Server, versions 3.1, 3.1.1, 4.1, 4.10.2, 4.11, or 4.12. The management server must be running one of the following operating systems:

- Red Hat Linux Advanced Server, version 2.1 (Update 3 for Red Hat Enterprise Linux AS, version 2.1, required)
- Red Hat Enterprise Linux AS, version 2.1 (Update 3 required)
- SUSE LINUX Enterprise Server 8 for x86 (Service Pack 3 required)
- Windows 2000, Server and Advanced Server (Service Pack 3 required)
- Windows Server 2003 (Standard, Enterprise, and Web Editions)

---

### Preparing to upgrade IBM Director Server on an xSeries server

Before you upgrade IBM Director Server, make sure that the instance of IBM Director Agent running on the management server will be fully functional and able to send alerts to IBM Director Server. This might require installing service processor device drivers or the IBM LM78 and SMBus device drivers for Linux.

#### Service processor device drivers

If you plan to upgrade IBM Director Server on an xSeries server that contains one of the following service processors, make sure that the service processor device driver has been installed:

- Advanced System Management processor
- Advanced System Management PCI Adapter
- Remote Supervisor Adapter
- Remote Supervisor Adapter II

If the device driver is not installed before you upgrade IBM Director Server, the power indications provider might not be installed. This component monitors power supplies and generates alerts in the event of failure.

#### IBM LM78 and SMBus device drivers for Linux

**Note:** If the IBM SMBus device driver, version 4.1, 4.11, or 4.12, is installed on the managed system, you must uninstall the device driver and then install the IBM SMBus device driver, version 4.20.

If you plan to upgrade IBM Director Server on an xSeries server running Linux, you might have to install either or both the LM78 and SMBus device drivers for Linux. These device drivers ensure that certain IBM Director tasks and functions work properly.

The following table contains information about these device drivers, when they must be installed, and what they do.

Table 22. Upgrading IBM Director Server: IBM LM78 and SMBus device drivers for Linux

Device driver	When it is needed	What it does
LM78	If either of the following conditions apply: <ul style="list-style-type: none"> <li>The server is an xSeries 225, machine type 8647 server.</li> <li>The server contains an integrated systems management processor (ISMP).</li> </ul>	The LM78 device driver ensures that IBM Director Server receives memory and processor PFA alerts.
SMBus	If the server does not contain one of the following service processors: <ul style="list-style-type: none"> <li>IPMI baseboard management controller</li> <li>Remote Supervisor Adapter</li> <li>Remote Supervisor Adapter II</li> </ul>	The SMBus device driver ensures that the Management Processor Assistant tasks and System Health Monitoring function properly.

## Downloading and installing the LM78 and SMBus device drivers

Perform the following steps to install either the IBM LM78 or SMBus device driver:

1. Uninstall the earlier version of the IBM SMBus device driver, if installed. Be sure to uninstall both the binary and source RPM files, if the source files were installed on the system.
2. Download the TAR.GZ file that contains the source RPM file from the IBM Web site
3. Build the binary RPM file
4. Install the binary RPM file on the system on which you will install IBM Director Server

### Uninstalling an earlier version of the IBM SMBus device driver

If the IBM SMBus device driver, version 4.1, 4.11, or 4.12, is installed on the managed system, you must uninstall the device driver before installing the IBM SMBus device driver, version 4.20.

Complete the following steps to uninstall the IBM SMBus device driver:

1. To uninstall the binary RPM file for the IBM SMBus device driver, from a command prompt, type the following command and press Enter:

```
rpm -e ibmsmb
```
2. To uninstall the source files for the IBM SMBus device driver, type the following command and press Enter:

```
rpm -e ibmsmb-src-distribution
```

where *distribution* is one of the following values:

- redhat for systems running Red Hat Linux or VMware ESX Server
- suse for systems running SUSE LINUX

## Downloading the IBM LM78 and SMBus device drivers

The following table provides information about the TAR.GZ files that contain the source RPM files for the LM78 and SMBus device drivers.

Table 23. Upgrading IBM Director Server: Source files for the LM78 and SMBus device drivers

Device driver	Operating system	File name
LM78	Red Hat Linux VMware ESX Server	dir4.20_lm78_redhatlinux.tar.gz
	SUSE LINUX	dir4.20_lm78_suselinux.tar.gz
SMBus	Red Hat Linux VMware ESX Server	dir4.20_smb_redhatlinux.tar.gz
	SUSE LINUX	dir4.20_smb_suselinux.tar.gz

You can download the files from the IBM Systems Management Software: Download/Electronic Support page at [http://www.ibm.com/pc/us/eserver/xseries/systems\\_management/dwnl.html](http://www.ibm.com/pc/us/eserver/xseries/systems_management/dwnl.html).

### Building the binary RPM file

You must build the binary RPM file on a system with the same kernel version and hardware configuration as the system on which you will install IBM Director Server. Make sure that the hardware configuration is similar in regard to the number of processors.

Complete the following steps to build either the LM78 or SMBus device driver:

1. Configure a system with the appropriate operating system and hardware configuration. Verify that the Linux kernel source is installed and properly configured.
2. Decompress the TAR.GZ file that contains the source RPM file.
3. To install the source RPM file, from a command prompt, type one of the following commands and press Enter:

<b>Red Hat Linux VMware ESX Server</b>	<code>rpm -ivh driver-src-redhat-4.20-1.i386.rpm</code>
<b>SUSE LINUX</b>	<code>rpm -ivh driver-src-suse-4.20-1.i386.rpm</code>

where *driver* is either `ibmlm78` or `ibmsmb`. This creates a binary RPM file in either the `/usr/local/ibmlm78` or the `/usr/local/smbus` directory, depending on which source RPM file you installed.

### Installing the IBM LM78 or SMBus device driver

**Note:** In this procedure, *driver* is one of the following strings:

<b>For the IBM LM78 device driver</b>	<code>ibmlm78</code>
<b>For the IBM SMBus device driver</b>	<code>ibmsmb</code>

Complete the following steps to install either the IBM LM78 or SMBus device driver:

1. If you built the binary RPM file on another server, create a `/usr/local/driver` directory on the server where you will install IBM Director Server. Copy the binary RPM file to that directory.
2. Change to the `/usr/local/driver` directory.

3. To install the device driver, from a command prompt, type the following command and press Enter:

```
rpm -ivh driver-4.20-1.i386.rpm
```

Issuing the command accomplishes the following tasks:

- Uncompresses and untars the archive into the `/usr/local/driver` directory
- Copies the device driver, shared library, and all configuration files to their appropriate locations
- Loads the device driver

---

## Upgrading IBM Director Server on Linux

This section provides instructions for upgrading IBM Director Server. When you upgrade IBM Director Server, the instances of IBM Director Console and IBM Director Agent that are running on the management server are upgraded automatically. All previously installed IBM Director Agent features and Server Plus Pack extension are upgraded also. You also can choose to install additional features and extensions.

**Note:** (Management server running SUSE LINUX only) If you plan to install Active PCI Manager and want to run the task against the management server, make sure that you have installed the necessary prerequisites. For more information, see Table 20, “IBM Active PCI Software necessary to run Active PCI Manager,” and Table 21, “Network adapter device drivers necessary to run the Fault Tolerant Management Interface,” on page 134.

Complete the following steps to upgrade IBM Director Server on Linux:

1. Insert the *IBM Director 4.20* CD into the CD-ROM drive.
2. If the CD does not automount, go to step 3. If the CD automounts, type the following command and press Enter:

```
umount /mnt/cdrom
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

3. Type the following command and press Enter:

```
mount -t iso9660 -o map=off /dev/cdrom /mnt/cdrom
```

where *dev/cdrom* is the specific device file for the CD-ROM block device and *mnt/cdrom* is mount point of the CD-ROM drive.

4. Change to the directory where the installation script is located. Type the following command and press Enter:

```
cd /mnt/cdrom/director/server/linux/i386/
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

5. If you want to customize the installation, go to step 6 on page 151. If you want to accept the default settings for the installation, type the following command and press Enter:

```
./dirinstall
```

Go to step 10 on page 151.

6. To customize the installation, copy the installation script to a local directory. Type the following command and press Enter:

```
cp dirinstall /directory/dirinstall
```

where *directory* is the local directory.

7. Open an ASCII text editor and modify the “User configuration” section of the dirinstall script. This file is fully commented.

You can specify the location of the Red Hat Package Manager (RPM) files, select previously uninstalled IBM Director extensions and features that you want to install, and select log file options.

8. Save the modified installation script.
9. To install IBM Director, type the following command and press Enter:

```
/directory/dirinstall
```

where *directory* is the local directory to which you copied the installation script.

10. To enable encryption or change security settings, type the following command and press Enter:

```
/opt/IBM/director/bin/cfgsecurity
```

11. To start IBM Director, type the following command and press Enter:

```
/opt/IBM/director/bin/twgstart
```

12. To unmount the CD-ROM drive, complete the following steps:

- a. Type `cd /` and press Enter.
- b. Type the following command and press Enter:

```
umount /mnt/cdrom
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

13. Remove the *IBM Director 4.20* CD from the CD-ROM drive.

To enable SNMP Access and Trap Forwarding, install and configure Net-SNMP, version 5.0.9. See “Enabling SNMP Access and Trap Forwarding for Linux” on page 198.

For instructions for installing IBM Director Software Distribution (Premium Edition) and the Rack Manager component, see “Completing the Rack Manager installation on the management server” on page 131 and “Installing Software Distribution (Premium Edition)” on page 132

---

## Upgrading IBM Director Server on Windows

### Notes:

1. If the following conditions apply, make sure that you have installed any necessary prerequisites:
  - The IBM Director Server installation either already includes Active PCI Manager or you plan to install Active PCI Manager.
  - You want to run the Active PCI Manager task against the management server.

For more information, see Table 20, “IBM Active PCI Software necessary to run Active PCI Manager,” and Table 21, “Network adapter device drivers necessary to run the Fault Tolerant Management Interface,” on page 134.

2. Early versions of Active PCI Manager are not compatible with IBM Director. Before you install IBM Director, make sure that you have uninstalled any Active PCI Manager, versions 1.0, 1.1, and 3.1.1, components.
3. (Scalable Systems Manager 4.11 or 4.12 installed only) If you do not plan to upgrade to Scalable Systems Manager (SSM) 4.20, uninstall SSM before upgrading to IBM Director Server 4.20. Otherwise, after the IBM Director Server upgrade is completed, you will not be able to uninstall SSM.

This section provides instructions for upgrading IBM Director Server. When you upgrade IBM Director Server, the instances of IBM Director Console and IBM Director Agent that are running on the management server are upgraded automatically. All previously installed IBM Director Agent features and Server Plus Pack extension are upgraded also. You also can choose to install additional features and extensions.

Complete the following steps to upgrade IBM Director Server on Windows:

1. Stop IBM Director Server. From a command prompt, type the following command and press Enter:

```
net stop twgipc
```
2. Close all applications, including any command-prompt windows.
3. Insert the *IBM Director 4.20* CD into the CD-ROM drive.
4. If the installation program starts automatically and the InstallShield wizard starts, go to step 6. Otherwise, click **Start** → **Run**.
5. In the **Open** field, type the following command and press Enter:

```
e:\setup.exe
```

where *e* is the drive letter of the CD-ROM drive. The installation program starts, and the “IBM Director” window opens.

6. Click **Install IBM Director**. The “IBM Director Installation” window opens.
7. Click **IBM Director Server installation**. The InstallShield wizard starts, and the “Welcome to the InstallShield Wizard” window opens.

If you are upgrading from IBM Director 3.10 or 3.1.1, the window is updated with the following message: IBM Director 3.x has been detected. The InstallShield Wizard might be slower than usual during the upgrade of the installation files.

8. Click **Next**. The “License Agreement” window opens.
9. Click **I accept the terms in the license agreement**; then, click **Next**. The “Server Plus Pack” window opens.



Figure 84. Upgrading IBM Director Server on Windows: “Server Plus Pack” window

10. Click **Next**. The “Feature and installation directory selection” window opens.

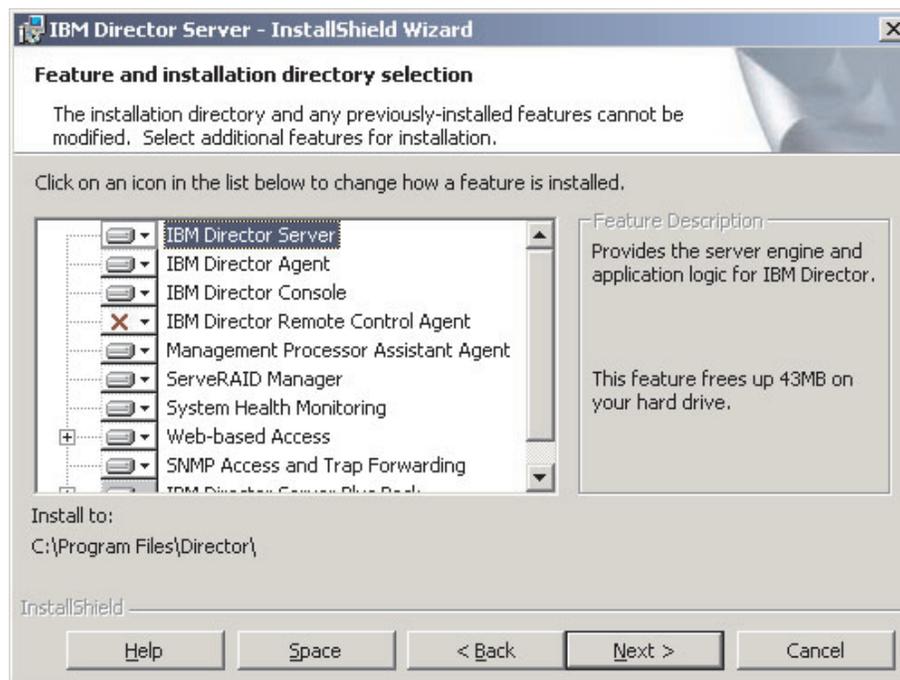


Figure 85. Upgrading IBM Director Server on Windows: “Feature and installation directory selection” window

IBM Director Server, IBM Director Agent, IBM Director Console, and any previously installed IBM Director Agent features are selected automatically for installation; a hard disk drive icon  is displayed to the left of each component.  is displayed to the left of the uninstalled features.

11. Select the IBM Director Agent features that you want to install:

**IBM Director Remote Control Agent**

Enables a system administrator to perform remote desktop functions on the management server

**Management Processor Assistant Agent**

Enables communication with service processors in IBM xSeries and Netfinity servers

**ServeRAID Manager**

Manages and monitors IBM ServeRAID adapters and integrated SCSI controllers with RAID capabilities

**System Health Monitoring**

Monitors the status of hardware components, produces and relays hardware alerts, and facilitates upward integration

**Web-based Access**

Enables system administrators to access the management-server data through a Web browser or the Microsoft Management Console (MMC)

**SNMP Access and Trap Forwarding**

Enables access to management-server data and alerts through SNMP

To select a feature, click  to the left of the feature name. A menu opens.

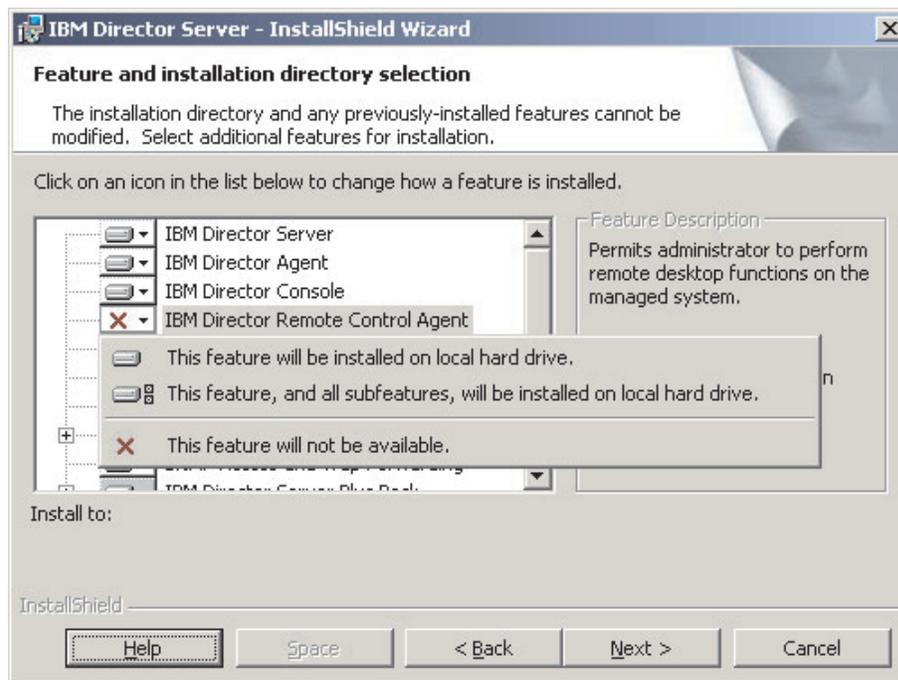


Figure 86. Upgrading IBM Director Server on Windows: “Feature and installation directory selection” window

To select the feature, click either **This feature will be installed on local hard drive** or **This feature, and all subfeatures, will be installed on local hard drive**.

12. Select the Server Plus Pack extensions that you want to install. Any previously installed Server Plus Pack extensions are selected automatically for installation. If they were not installed previously, you can select the following extensions:

**Capacity Manager**

Tracks system resource utilization, identifies bottlenecks, and provides performance information

**Rack Manager**

Manages IBM servers, storage devices, and other components in an IBM enclosure

**Active PCI Manager**

Manages PCI and PCI-X adapters in managed systems

**Software Rejuvenation**

Schedules restarts of managed systems

**System Availability**

Determines availability of managed systems and provides statistical data

To select the complete Server Plus Pack, click the icon to the left of **IBM Director Server Plus Pack**; then, click **This feature, and all subfeatures, will be installed on local hard drive**. Otherwise, select the Server Plus Pack extensions individually.

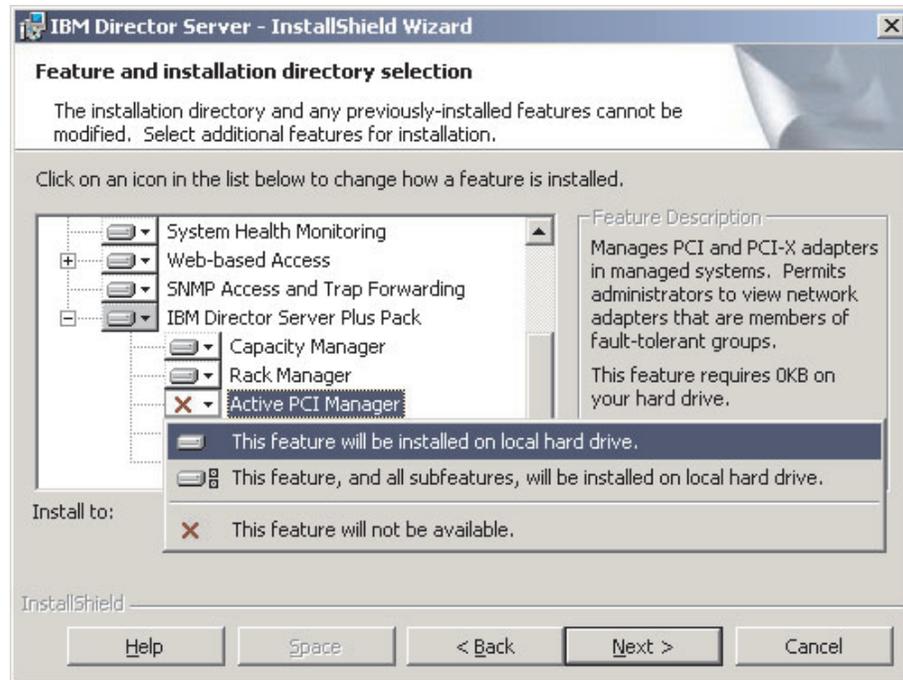


Figure 87. Upgrading IBM Director Server on Windows: Installing the Server Plus Pack

**Notes:**

- a. Rack Manager will not function until the Rack Manager component, which is on the *IBM Director Server Plus Pack* CD, is installed on the management server.
  - b. Until you install the Server Plus Pack extensions on the managed systems, you can run the Server Plus Pack tasks only against the management server.
13. Click **Next**. The “IBM Director service account information” window opens. For more information, see “IBM Director service account (Windows only)” on page 32.



Figure 88. Upgrading IBM Director Server on Windows: “IBM Director service account information” window

14. Type information about the service account used for the existing IBM Director Server installation:
- a. In the **Local computer name or domain** field, type the computer name of the IBM Director service account. If the service account is a domain account, type the domain.
  - b. In the **User Name** field, type the user ID for the IBM Director service account.
  - c. In the **Password** and **Confirm Password** fields, type the password for the IBM Director service account.

**Note:** Do not change the service account information. If you do, the installation will fail.

15. Click **Next**. The “Encryption settings” window opens.

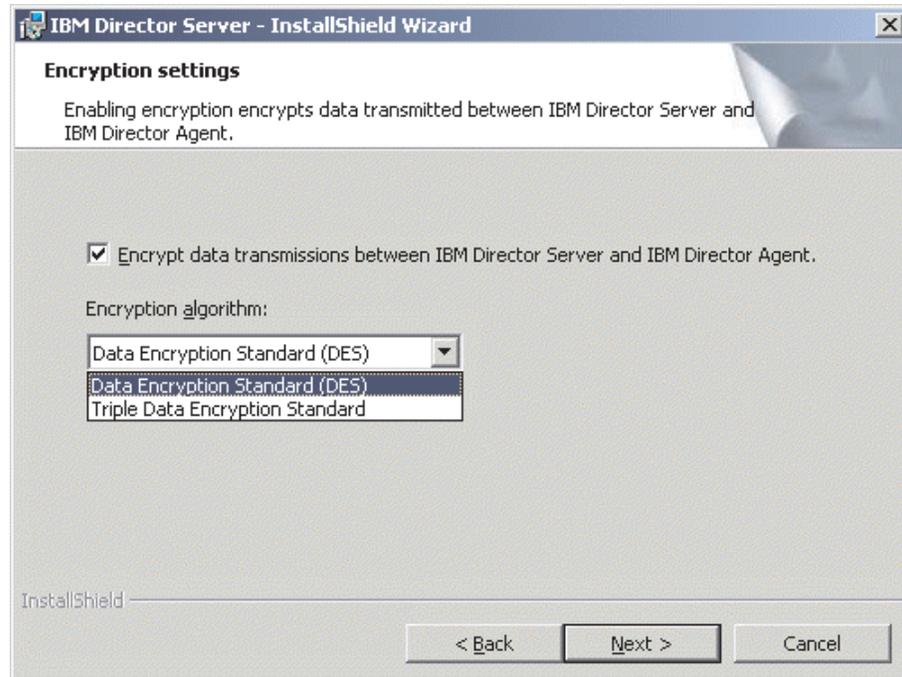


Figure 89. Installing IBM Director Server on Windows: “Encryption settings” window

16. To encrypt data transmitted between IBM Director Server and IBM Director Agent, select the **Encrypt data transmissions between IBM Director Server and IBM Director Agent** check box; then, select the encryption algorithm.
17. Click **Next**. The “Software-distribution settings” window opens.

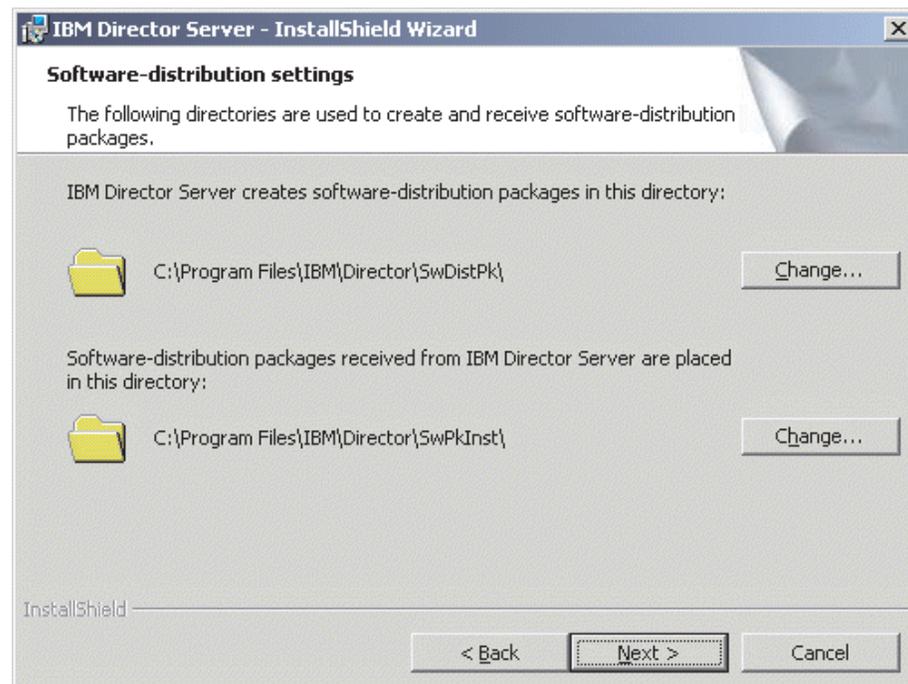


Figure 90. Upgrading IBM Director Server on Windows: “Software-distribution settings” window

18. Click **Next**. If you did not select to install the Web-based Access feature, the “Ready to Install the Program” window opens; go to step 20. Otherwise, the “Web-based Access information” window opens.

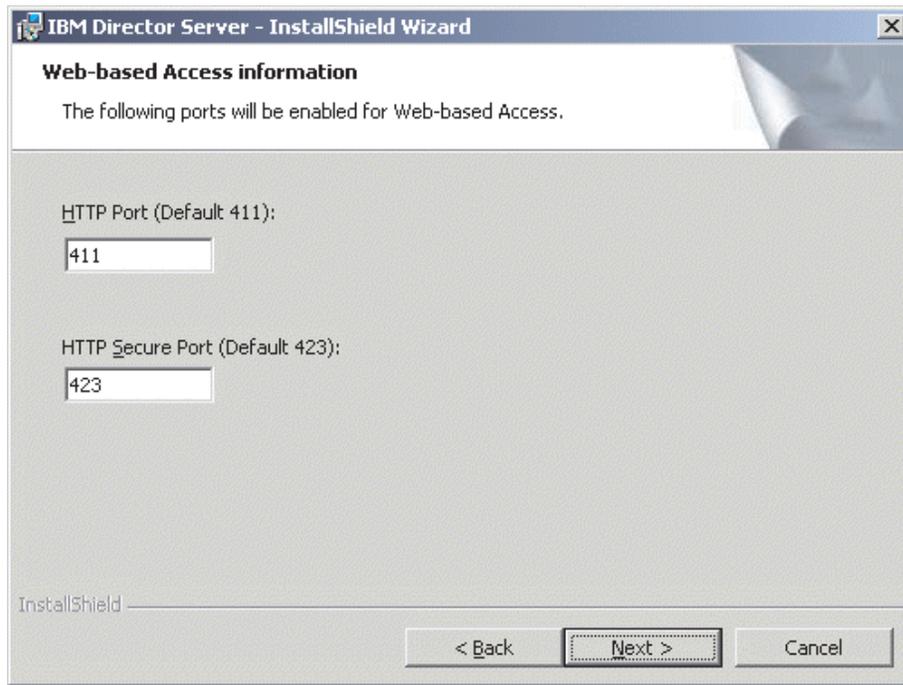


Figure 91. Upgrading IBM Director Server on Windows: “Web-based Access information” window

19. Change the default HTTP ports (if necessary); then, click **Next**. The “Ready to Install the Program” window opens.
20. Click **Install**. The “Installing IBM Director Server” window opens. The progress of the installation is displayed in the **Status** field. When the installation is completed, the “Network driver configuration” window opens.

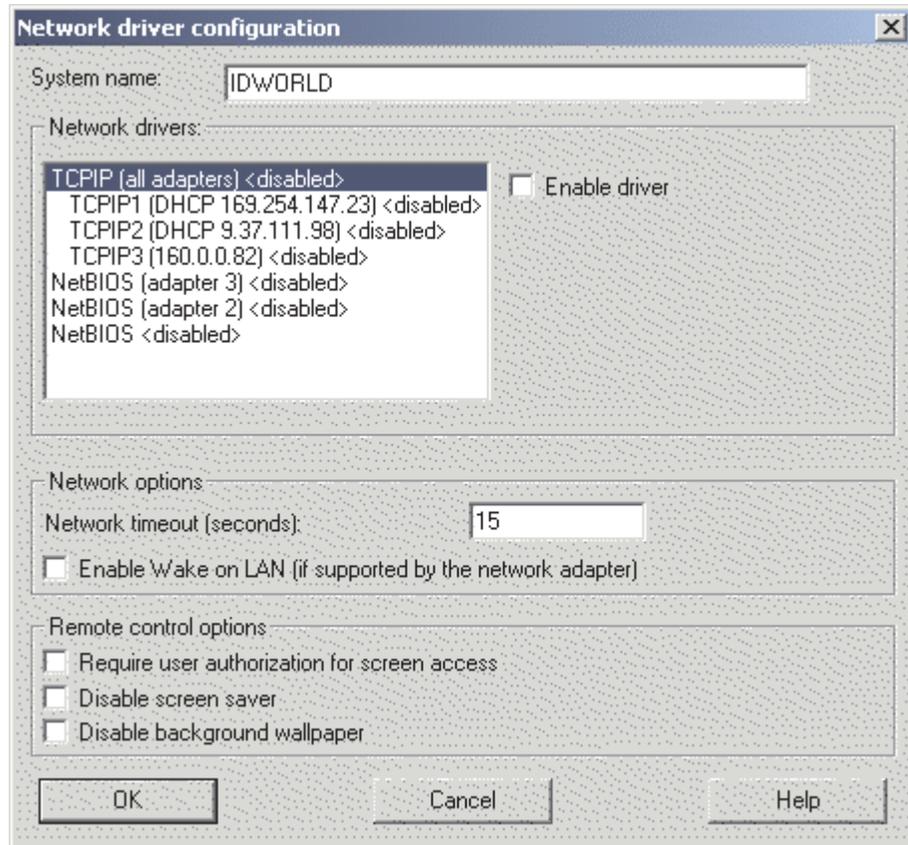


Figure 92. Upgrading IBM Director Server on Windows: “Network driver configuration” window

21. In the **System name** field, type the name that you want to be displayed in IBM Director Console. By default, this is the NetBIOS name of the management server.
22. Define the communications protocols to use for communication between IBM Director Server and IBM Director Agent:
  - a. In the **Network drivers** field, TCPIP (all adapters) is enabled by default. To enable another protocol, select the protocol and then select the **Enable driver** check box.

**Note:** If you disable TCPIP (all adapters) and enable an individual device driver on a system with multiple network adapters, IBM Director Server will receive *only* those data packets addressed to the individual adapter.

- b. In the **Network timeout** field, type the number of seconds that IBM Director Server waits for a response from IBM Director Agent. By default, this is set to 15 seconds.
- c. Select the **Enable Wake on LAN** check box if the network adapter supports the Wake on LAN feature.

**Note:** To determine whether your server supports the Wake on LAN feature, see your server documentation.

23. If you selected to install the IBM Director Remote Control Agent, the following options are available:

**Require user authorization for system access**

Select this check box to request authorization from the local user before controlling the management server remotely.

**Disable screen saver**

Select this check box to disable the screen saver when the management server is controlled remotely.

**Disable background wallpaper**

Select this check box to disable desktop wallpaper when the management server is controlled remotely. You might want to disable the wallpaper because complicated backgrounds slow down remote control and increase network traffic.

24. Click **OK**. The status bar displays the progress of the installation. When the installation is completed, the “InstallShield Wizard Completed” window opens.
25. Click **Finish**. A window opens, asking you if you want to restart the server.
26. Remove the *IBM Director 4.20* CD from the CD-ROM drive.
27. Click **Yes** to restart the server.

For instructions for installing IBM Director Software Distribution (Premium Edition) and the Rack Manager component, see “Completing the Rack Manager installation on the management server” on page 131 and “Installing Software Distribution (Premium Edition)” on page 132

---

## Chapter 11. Upgrading IBM Director Console

This chapter contains instructions for upgrading IBM Director Console.

You can upgrade to IBM Director Console 4.20 from IBM Director Console, versions 3.1, 3.1.1, 4.1, 4.10.2, 4.11, or 4.12. The management console must be running one of the following operating systems:

- Red Hat Linux Advanced Server, version 2.1 (Update 3 for Red Hat Enterprise Linux AS, version 2.1, required)
- Red Hat Enterprise Linux AS, version 2.1 (Update 3 required)
- SUSE LINUX Enterprise Server 8 for x86 (Service Pack 3 required)
- Windows Server 2003, Enterprise, Standard, and Web Editions
- Windows 2000 Professional, Server, and Advanced Server (Service Pack 3 required)
- Windows XP Professional (Service Pack 1 recommended)

---

### Upgrading IBM Director Console on Linux

This section contains instructions for upgrading IBM Director Console using the *IBM Director 4.20* CD. It also contains instructions for upgrading IBM Director Console and IBM Director Agent simultaneously.

When you upgrade IBM Director Console, IBM Director automatically upgrades all previously installed IBM Director features and Server Plus Pack extensions. You also can choose to install additional features and extensions.

**Notes:**

1. IBM Director Console is not supported on the Gnome desktop environment.
2. If the management console also has IBM Director Agent installed, you *must* perform the upgrade using the instructions in “Upgrading IBM Director Console and IBM Director Agent simultaneously” on page 162.

### Upgrading IBM Director Console

Complete the following steps to upgrade IBM Director Console on Linux:

1. Insert the *IBM Director 4.20* CD into the CD-ROM drive.
2. If the CD does not automount, go to step 3. If the CD automounts, type the following command and press Enter:

```
umount /mnt/cdrom
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

3. Type the following command and press Enter:

```
mount -t iso9660 -o map=off /dev/cdrom /mnt/cdrom
```

where *dev/cdrom* is the specific device file for the CD-ROM block device and *mnt/cdrom* is mount point of the CD-ROM drive.

4. Change to the directory where the installation script is located. Type the following command and press Enter:

```
cd /mnt/cdrom/director/console/linux/i386/
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

5. Copy the installation script to a local directory. Type the following command and press Enter:

```
cp dirinstall /directory/dirinstall
```

where *directory* is the local directory.

6. Open an ASCII text editor and modify the “User configuration” section of the dirinstall script. This file is fully commented.

You can specify the location of the RPM files, select previously uninstalled IBM Director extensions and features that you want to install, and select log file options.

7. Save the modified installation script.

8. To install IBM Director, type the following command and press Enter:

```
/directory/dirinstall
```

where *directory* is the local directory to which you copied the installation script.

9. To unmount the CD-ROM drive, complete the following steps:

- a. Type `cd /` and press Enter.

- b. Type the following command and press Enter:

```
umount /mnt/cdrom
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

10. Remove the *IBM Director 4.20* CD from the CD-ROM drive.

## Upgrading IBM Director Console and IBM Director Agent simultaneously

### Notes:

1. Make sure that the operating-system password-encryption method is set to message digest 5 (MD5) or DES.
2. If you want to use the Remote Session task on the managed system, make sure that the package that contains telnetd is installed and configured. This is usually in the `telnet_server_version.i386.RPM` package, where *version* is the code level of your Linux distribution.

Complete the following steps to upgrade IBM Director Console and IBM Director Agent at the same time:

1. Download `dir4.20_agentconsoleupgrade_linux.tar.gz` from the IBM Systems Management Software: Download/Electronic Support page at [http://www.ibm.com/pc/us/eserver/xseries/systems\\_management/dwnl.html](http://www.ibm.com/pc/us/eserver/xseries/systems_management/dwnl.html).
2. Decompress the TAR.GZ file. It contains the following file:  
`IBMDirectorAgentConsolePatch4.20-1.sh`.
3. (Optional) To save the RPM files, from a command prompt, type the following command and press Enter:

```
./IBMDirectorAgentConsolePatch4.20-1.sh -x directory
```

where *directory* is the fully qualified file name of the directory to which the RPM files are written.

4. To install IBM Director Console and IBM Director Agent, type the following command and press Enter:

```
./IBMDirectorAgentConsolePatch4.20-1.sh
```

---

## Upgrading IBM Director Console on Windows

This section provides instructions for upgrading IBM Director Console using the InstallShield wizard. The wizard can be used in a standard interactive mode, or you can perform an unattended installation using a response file to provide answers to the questions that the wizard poses.

When you upgrade IBM Director Console, IBM Director automatically upgrades all previously installed IBM Director features and Server Plus Pack extensions. You also can choose to install additional features and extensions.

### Notes:

1. Early versions of Active PCI Manager are not compatible with IBM Director. Before you upgrade IBM Director, make sure that you have uninstalled any Active PCI Manager, versions 1.0, 1.1, and 3.1.1, components.
2. (Scalable Systems Manager 4.11 or 4.12 installed only) If you do not plan to upgrade to Scalable Systems Manager (SSM) 4.20, uninstall SSM before upgrading to IBM Director Console 4.20. Otherwise, after the IBM Director Console upgrade is completed, you will not be able to uninstall SSM.
3. If you have both IBM Director Console and IBM Director Agent installed on a system, you *must* upgrade both components. After you upgrade IBM Director Console, upgrade IBM Director Agent. See “Upgrading IBM Director Agent on Windows (32-bit)” on page 175.

## Upgrading IBM Director Console using the InstallShield wizard

Complete the following steps to upgrade IBM Director Console on Windows:

1. If IBM Director Agent is installed, from a command prompt, type the following command and press Enter:  

```
net stop twgipc
```
2. Close all open applications, including command-prompt sessions.
3. Insert the *IBM Director 4.20* CD into the CD-ROM drive.
4. If the installation program starts automatically and the InstallShield wizard starts, go to step 6. Otherwise, click **Start** → **Run**.
5. In the **Open** field, type the following command and press Enter:  

```
e:\setup.exe
```

where *e* is the drive letter of the CD-ROM drive. The installation program starts, and the “IBM Director” window opens.

6. Click **Install IBM Director**. The “IBM Director Installation” window opens.
7. Click **IBM Director Console installation**. The “Welcome to the InstallShield Wizard” window opens.

If you are upgrading from IBM Director 3.10 or 3.11, the window is updated with the following message: IBM Director 3.x has been detected. The InstallShield Wizard might be slower than usual during the upgrade of the installation files.

8. Click **Next**. The “License Agreement” window opens.
9. Click **I accept the terms in the license agreement**; then, click **Next**. The “Server Plus Pack” window opens.



Figure 93. Upgrading IBM Director Console: "Server Plus Pack" window

10. Click **Next**. The "Feature and installation directory selection" window opens.

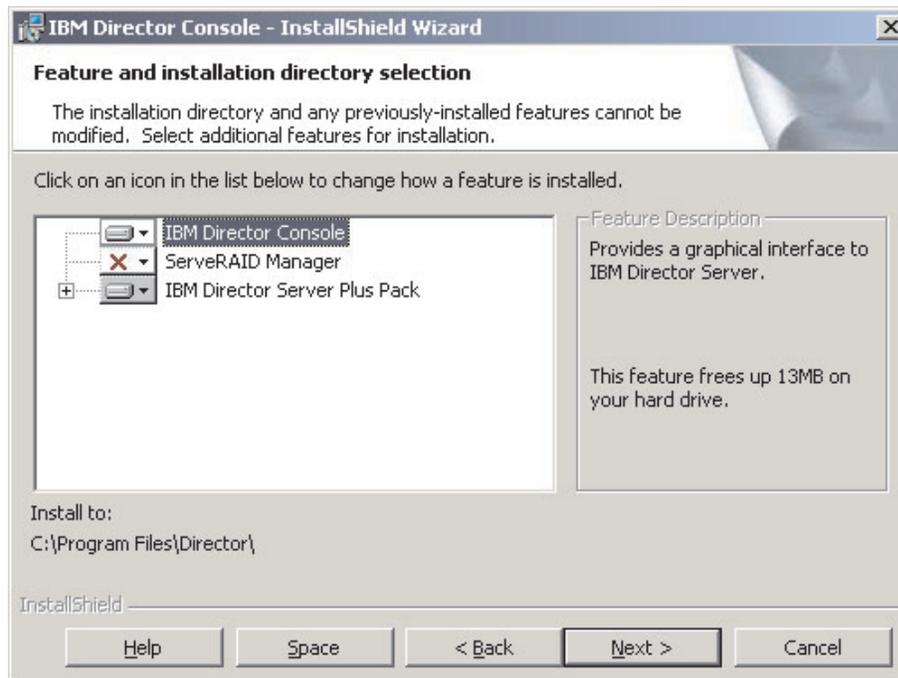


Figure 94. Upgrading IBM Director Console: "Feature and destination directory selection" window

IBM Director Console and any previously installed features are selected automatically for installation; a hard disk drive icon  is displayed to the left of the component.  is displayed to the left of the uninstalled features.

If it was not installed previously, you can install ServeRAID Manager, a feature that manages and monitors IBM ServeRAID adapters.

11. To select ServeRAID Manager, click  to the left of the feature name. A menu opens. Click **This feature will be installed on local hard drive.**

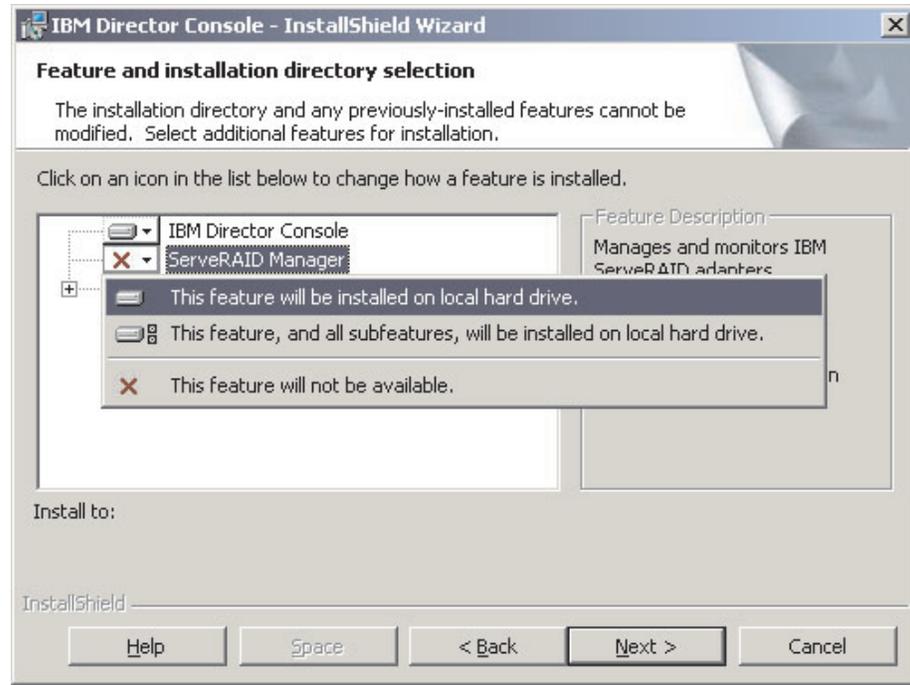


Figure 95. Upgrading IBM Director Console: Installing ServeRAID Manager

12. Select the Server Plus Pack extensions that you want to install:

**Capacity Manager**

Tracks system resource utilization, identifies bottlenecks, and provides performance information

**Rack Manager**

Manages IBM servers, storage devices, and other components in an IBM enclosure

**Active PCI Manager**

Manages PCI and PCI-X adapters in managed systems

**Software Rejuvenation**

Schedules restarts of managed systems

**System Availability**

Determines availability of managed systems and provides statistical data

To select the complete Server Plus Pack, click the icon to the left of **IBM Director Server Plus Pack**; then, click **This feature, and all subfeatures, will be installed on local hard drive.** Otherwise, select the Server Plus Pack extensions individually.

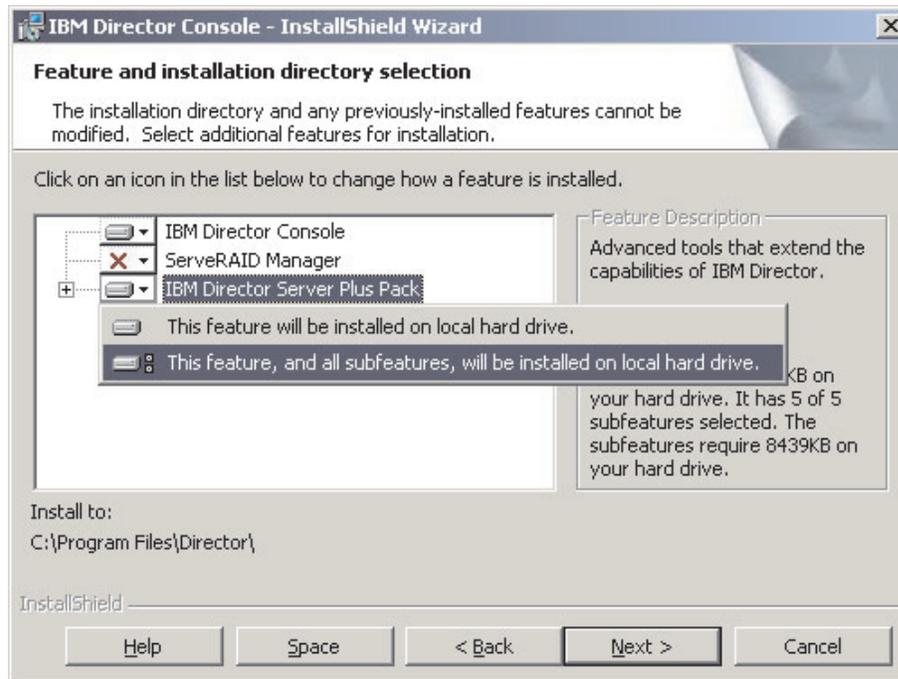


Figure 96. Upgrading IBM Director Console: Installing the Server Plus Pack

**Notes:**

- a. Rack Manager will not function until the Rack Manager component, which is on the *IBM Director Server Plus Pack* CD, is installed on the management server.
  - b. Until you install the Server Plus Pack extensions on the managed systems, you can run the Server Plus Pack tasks only against the management server.
13. Click **Next**. The “Ready to Install the Program” window opens.
  14. Click **Install**. The “Installing IBM Director Console” window opens. The status bar displays the progress of the installation. When the installation is completed, the “InstallShield Wizard Completed” window opens.
  15. Click **Finish**. A window opens, asking if you want to restart the system.
  16. Remove the *IBM Director 4.20* CD from the CD-ROM drive.
  17. Click **Yes** to restart the system.

## Performing an unattended upgrade of IBM Director Console

You can perform an unattended upgrade of IBM Director Console using a response file, which provides answers to the questions that are posed by the InstallShield wizard.

Complete the following steps to upgrade IBM Director Console on Windows:

1. If IBM Director Agent is installed, from a command prompt, type the following command and press Enter:  

```
net stop twgipc
```
2. Close all open applications, including command-prompt sessions.
3. Insert the *IBM Director 4.20* CD into the CD-ROM drive.
4. Copy the dircon.rsp file to a local directory. This file is in the director\console\windows\i386 directory on the *IBM Director 4.20* CD.

5. From Windows Explorer, right-click the copy of the `dircon.rsp` file and then click **Properties**. The “`dircon.rsp Properties`” window opens. Clear the **Read-Only** check box and click **OK**.
6. Open the copy of the `dircon.rsp` file in an ASCII text editor.
7. Modify and save the `dircon.rsp` file. This file follows the Windows INI file format and is fully commented.

**Note:** Windows automatically detects and upgrades the IBM Director features that were part of the existing IBM Director installation. However, you can select features that were not installed previously.

8. Change to the directory that contains the IBM Director Console installation file (`ibmsetup.exe`). This file is in the `director\console\windows\i386` directory on the *IBM Director 4.20* CD.
9. From the command prompt, type the following command and press Enter:  
`ibmsetup.exe installationtype rsp="responsefile.rsp"`

where:

- *installationtype* is one of the following commands:
    - **unattended** shows the progress of the installation but does not require any user input.
    - **silent** suppresses all output to the screen during installation.
  - *responsefile.rsp* is the path and name of the response file that you created in step 7.
10. When the installation is completed, remove the *IBM Director 4.20* CD from the CD-ROM drive.



---

## Chapter 12. Upgrading IBM Director Agent

This chapter contains instructions for upgrading IBM Director Agent.

You can upgrade to IBM Director Agent 4.20 from IBM Director Agent, versions 3.1, 3.1.1, 4.1, 4.10.2, 4.11, or 4.12. You can use either standard installation procedures or the IBM Director Software Distribution task. The managed system must be running a supported operating system. See “Supported operating systems” on page 14 for more information.

If you want to use IBM Director 4.20 to manage a system running an operating system that IBM Director 4.20 does not support, do not upgrade IBM Director Agent. IBM Director 4.20 can manage systems running IBM Director Agent, versions 3.1, 3.1.1, 4.1, 4.10.2, 4.11, 4.12, or 4.20.

---

### Preparing to upgrade IBM Director Agent on an xSeries server

Before you upgrade IBM Director Agent, make sure that you have installed all necessary device drivers. This might require installing service processor device drivers or the IBM LM78 and SMBus device drivers for Linux.

#### Service processor device drivers

If you plan to upgrade IBM Director Agent on an xSeries server that contains one of the following service processors, make sure that the service processor device driver has been installed:

- Advanced System Management processor
- Advanced System Management PCI Adapter
- Remote Supervisor Adapter
- Remote Supervisor Adapter II

If the device driver is not installed before you upgrade IBM Director Agent, the power indications provider might not be installed. This component monitors power supplies and generates alerts in the event of failure.

#### IBM LM78 and SMBus device drivers for Linux

**Note:** If the IBM SMBus device driver, version 4.1, 4.11, or 4.12, is installed on the managed system, you must uninstall the device driver and then install the IBM SMBus device driver, version 4.20.

If you plan to upgrade IBM Director Agent on an xSeries server running Linux, you might have to install either or both the LM78 and SMBus device drivers for Linux. These device drivers ensure that certain IBM Director tasks and functions work properly.

The following table contains information about these device drivers, when they must be installed, and what they do.

Table 24. Upgrading IBM Director Agent: IBM LM78 and SMBus device drivers for Linux

Device driver	When it is needed	What it does
LM78	If either of the following conditions apply: <ul style="list-style-type: none"> <li>The server is an xSeries 225, machine type 8647 server.</li> <li>The server contains an integrated systems management processor (ISMP).</li> </ul>	The LM78 device driver ensures that IBM Director Server receives memory and processor PFA alerts.
SMBus	If the server does not contain one of the following service processors: <ul style="list-style-type: none"> <li>IPMI baseboard management controller</li> <li>Remote Supervisor Adapter</li> <li>Remote Supervisor Adapter II</li> </ul>	The SMBus device driver ensures that the Management Processor Assistant tasks and System Health Monitoring function properly.

## Downloading and installing the LM78 and SMBus device drivers

Complete the following steps to install either the IBM LM78 or SMBus device driver:

1. Uninstall the earlier version of the IBM SMBus device driver, if installed. Be sure to uninstall both the binary and source RPM files, if the source files were installed on the system.
2. Download the TAR.GZ file that contains the source RPM file from the IBM Web site.
3. Build the binary RPM file.
4. Install the binary RPM file on the system on which you will install IBM Director Agent.

### Uninstalling an earlier version of the IBM SMBus device driver

If the IBM SMBus device driver, version 4.1, 4.11, or 4.12, is installed on the managed system, you must uninstall the device driver before installing the IBM SMBus device driver, version 4.20.

Complete the following steps to uninstall the IBM SMBus device driver:

1. To uninstall the binary RPM file for the IBM SMBus device driver, from a command prompt, type the following command and press Enter:

```
rpm -e ibmsmb
```
2. To uninstall the source files for the IBM SMBus device driver, type the following command and press Enter:

```
rpm -e ibmsmb-src-distribution
```

where *distribution* is one of the following values:

- redhat for systems running Red Hat Linux or VMware ESX Server
- suse for systems running SUSE LINUX

## Downloading the IBM LM78 and SMBus device drivers

The following table provides information about the TAR.GZ files that contain the source RPM files for the LM78 and SMBus device drivers.

Table 25. Upgrading IBM Director Agent: Source files for the LM78 and SMBus device drivers

Device driver	Operating system	File name
LM78	Red Hat Linux VMware ESX Server	dir4.20_lm78_redhatlinux.tar.gz
	SUSE LINUX	dir4.20_lm78_suselinux.tar.gz
SMBus	Red Hat Linux VMware ESX Server	dir4.20_smb_redhatlinux.tar.gz
	SUSE LINUX	dir4.20_smb_suselinux.tar.gz

You can download the files from the IBM Systems Management Software: Download/Electronic Support page at [http://www.ibm.com/pc/us/eserver/xseries/systems\\_management/dwnl.html](http://www.ibm.com/pc/us/eserver/xseries/systems_management/dwnl.html).

### Building the binary RPM file

You must build the binary RPM file on a system with the same kernel version and hardware configuration as the system on which you will install IBM Director Agent. Make sure that the hardware configuration is similar in regard to the number of processors.

Complete the following steps to build either the LM78 or SMBus device driver:

1. Configure a system with the appropriate operating system and hardware configuration. Make sure that the Linux kernel source is installed and properly configured.
2. Decompress the TAR.GZ file that contains the source RPM file.
3. To install the source RPM file, from a command prompt, type one of the following commands and press Enter:

<b>Red Hat Linux and VMware ESX Server</b>	<code>rpm -ivh driver-src-redhat-4.20-1.i386.rpm</code>
<b>SUSE LINUX</b>	<code>rpm -ivh driver-src-suse-4.20-1.i386.rpm</code>

where *driver* is either *ibmlm78* or *ibmsmb*. This creates a binary RPM file in either the `/usr/local/lm78` or `/usr/local/ibmsmb` directory, depending on which source RPM file you installed.

### Installing the IBM LM78 or SMBus device driver

**Note:** In this procedure, *driver* is one of the following strings:

<b>For the IBM LM78 device driver</b>	<code>ibmlm78</code>
<b>For the IBM SMBus device driver</b>	<code>ibmsmb</code>

Complete the following steps to install either the IBM LM78 or SMBus device driver:

1. If you built the binary RPM file on another server, create a `/usr/local/ibm/driver` directory on the server where you will install IBM Director Agent. Copy the binary RPM file to that directory.
2. Change to the `/usr/local/driver` directory.

3. To install the device driver, from a command prompt, type the following command and press Enter:

```
rpm -ivh driver-4.20-1.i386.rpm
```

Issuing the command accomplishes the following tasks:

- Uncompresses and untars the archive into the `/usr/local/driver` directory
- Copies the device driver, shared library, and all configuration files to the applicable locations
- Loads the device driver

---

## Upgrading IBM Director Agent using standard installation procedures

This section contains information about upgrading IBM Director Agent using standard installation procedures.

### Upgrading IBM Director Agent on Linux

#### Notes:

1. If the managed system also has IBM Director Console installed, you must perform the upgrade using the instructions in “Upgrading IBM Director Console and IBM Director Agent simultaneously” on page 162.
2. Make sure that the operating-system password-encryption method is set to message digest 5 (MD5) or DES.
3. If you want to use the Remote Session task on the managed system, make sure that the package that contains telnetd is installed and configured. This is usually in the `telnet_server_version.i386.RPM` package, where *version* is the code level of your Linux distribution.
4. The support for installing IBM Director Agent on operating systems for IBM iSeries and pSeries is only available only through the IBM Virtualization Engine and the *IBM Director 4.20* CD shipped with certain BladeCenter chassis. You also can download the software that is available on that CD from the IBM Support Web site.

When you upgrade IBM Director Agent, IBM Director automatically upgrades all previously installed IBM Director features. You can also choose to install additional features.

Complete the following steps to upgrade to IBM Director Agent on Linux:

1. Stop IBM Director Agent. From a command prompt, type the following command and press Enter:

```
/opt/Variable/director/bin/twgstop
```

where *Variable* is one of the following strings:

---

<b>For 32-bit operating systems or operating systems for AMD64</b>	IBM
--	-----

---

<b>For operating systems for Intel Itanium and IBM iSeries and IBM pSeries</b>	ibm
--	-----

---

2. Insert the *IBM Director 4.20* CD into the CD-ROM drive.

3. If the CD does not automount, go to step 4. If the CD automounts, type the following command and press Enter:

```
umount /mnt/cdrom
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

4. Type the following command and press Enter:

```
mount -t iso9660 -o map=off /dev/cdrom /mnt/cdrom
```

where *dev/cdrom* is the specific device file for the CD-ROM block device and *mnt/cdrom* is mount point of the CD-ROM drive.

5. Change to the directory where the installation script is located. Type the following command and press Enter:

```
cd /mnt/cdrom/director/agent/linux/location/
```

where *mnt/cdrom* is the mount point of the CD-ROM drive, and *location* is one of the following strings:

---

<b>For 32-bit operating systems or operating systems for AMD64</b>	i386
<b>For operating systems for Intel Itanium</b>	ia64
<b>For operating systems for IBM iSeries and IBM pSeries</b>	ppc

---

6. Copy the installation script to a local directory. Type the following command and press Enter:

```
cp dirinstall /directory/dirinstall
```

where *directory* is the local directory.

7. Open an ASCII text editor and modify the “User configuration” section of the *dirinstall* script. This file is fully commented.

You can specify the location of the RPM files, select previously uninstalled IBM Director Agent features that you want to install, and select log file options.

8. Save the modified installation script.

9. To install IBM Director, type the following command and press Enter:

```
/directory/dirinstall
```

where *directory* is the local directory to which you copied the installation script.

10. To enable encryption or change security settings, type the following command and press Enter:

```
/opt/Variable/director/bin/cfgsecurity
```

where *Variable* is one of the following strings:

---

<b>For 32-bit operating systems or operating systems for AMD64</b>	IBM
<b>For operating systems for IBM iSeries and IBM pSeries</b>	ibm

---

**Note:** Encryption is not supported on managed systems running either of the following operating systems:

- Red Hat Enterprise Linux AS, version 3.0, for Intel Itanium
- SUSE LINUX Enterprise Server 8 for Itanium Processor Family

11. To start IBM Director Agent, type the following command and press Enter:  
`/opt/Variable/director/bin/twgstart`

where *Variable* is one of the following strings:

---

<b>For 32-bit operating systems or operating systems for AMD64</b>	IBM
--	-----

---

<b>For operating systems for Intel Itanium and IBM iSeries and IBM pSeries</b>	ibm
--	-----

---

12. To unmount the CD-ROM drive, complete the following steps:

- Type `cd /` and press Enter.
- Type the following command and press Enter:

```
umount /mnt/cdrom
```

where *mnt/cdrom* is the mount point of the CD-ROM drive.

13. Remove the *IBM Director 4.20* CD from the CD-ROM drive.

After IBM Director Agent is installed, you can enable the Wake on LAN feature. See “Enabling the Wake on LAN feature” on page 198

To enable SNMP Access and Trap Forwarding, you must install and configure Net-SNMP, version 5.0.9. See “Enabling SNMP Access and Trap Forwarding for Linux” on page 198.

For information about installing the IBM Director Server Plus Pack extensions, see Chapter 9, “Installing IBM Director extensions,” on page 131

## Upgrading IBM Director Agent on NetWare

When you upgrade IBM Director Agent, IBM Director automatically upgrades all previously installed IBM Director features. You also can choose to install additional features.

Complete the following steps to upgrade IBM Director Agent on NetWare:

1. On the NetWare server, change to the console screen.
2. Stop IBM Director Agent. From the console, type the following command and press Enter:  
`unload twgipc`
3. Insert the *IBM Director 4.20* CD into the CD-ROM drive of the system running Windows. If the autorun window opens, close it.
4. Start Windows Explorer and open the `\director\agent\netware` directory.
5. Double-click **setup.exe**. The InstallShield wizard starts, and the “Welcome to the InstallShield Wizard” window opens.
6. Click **Next**. The “Installing IBM Director Agent” window opens.
7. Click **Yes** to accept the license agreement. A warning window opens, stating that an existing version of IBM Director has been detected.
8. Click **OK**. The “Choose destination location” window opens.

- Click the drive that is mapped to the SYS volume on the NetWare server; then, click **Next**. The “Select Components” window opens.

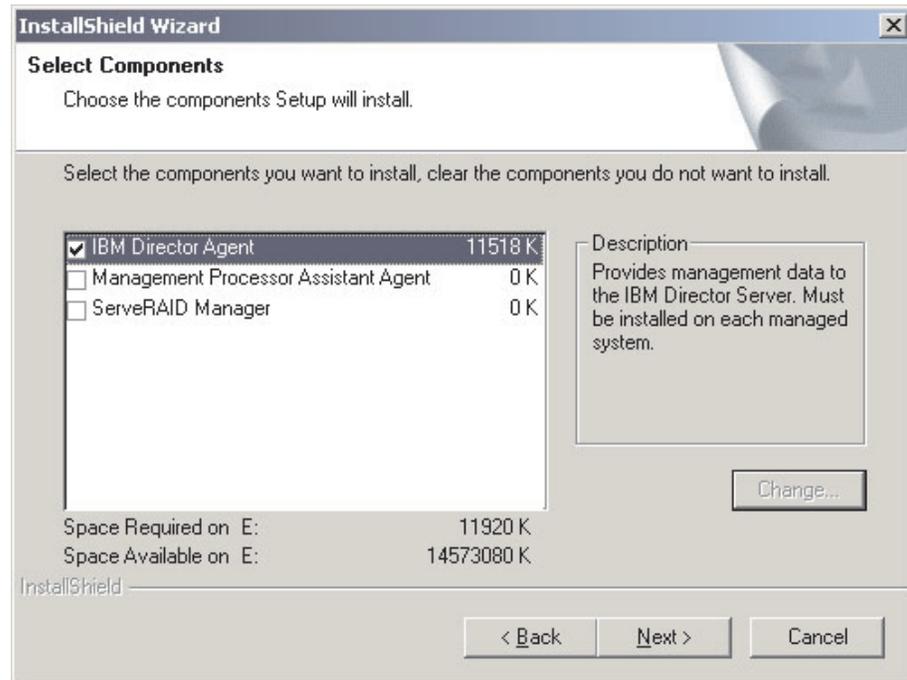


Figure 97. Upgrading IBM Director Agent on NetWare: “Select Components” window

- Select the check boxes for the previously-uninstalled features you want to install; then, click **Next**. A status bar displays the progress of the installation. When the installation is completed, the “InstallShield Wizard Complete” window opens.
- Click **Finish**.
- Remove the *IBM Director 4.20* CD from the CD-ROM drive.
- On the server running NetWare, start IBM Director Agent. Type the following command and press Enter:

```
load twgipc
```

For information about installing the IBM Director Server Plus Pack extensions, see Chapter 9, “Installing IBM Director extensions,” on page 131

## Upgrading IBM Director Agent on Windows (32-bit)

This section provides information about installation prerequisites and instructions for upgrading IBM Director Agent using the InstallShield wizard. The wizard can be used in a standard interactive mode, or you can perform an unattended installation using a response file to provide answers to the questions that the wizard poses.

When you upgrade IBM Director Agent, IBM Director automatically upgrades all previously-installed IBM Director features. You also can choose to install additional features.

### Notes:

- Early versions of Active PCI Manager are not compatible with IBM Director. Before you upgrade IBM Director, make sure that you have uninstalled any Active PCI Manager, versions 1.0, 1.1, and 3.1.1, components.

2. If you have both IBM Director Agent and IBM Director Console installed on a system, you *must* upgrade both components. If you have not done so already, upgrade to IBM Director Console 4.1 before upgrading to IBM Director Agent 4.1. See Chapter 11, “Upgrading IBM Director Console,” on page 161.

## Upgrading IBM Director Agent using the InstallShield wizard

Complete the following steps to upgrade IBM Director Agent on Windows:

1. Stop IBM Director Agent. From a command prompt, type the following command and press Enter:

```
net stop twgipc
```

2. Close all applications, including any command-prompt sessions.
3. Insert the *IBM Director 4.20* CD into the CD-ROM drive.
4. If the installation program starts automatically and the InstallShield wizard starts, go to step 6. Otherwise, click **Start** → **Run**.
5. In the **Open** field, type the following command and press Enter:

```
e:\setup.exe
```

where *e* is the drive letter of the CD-ROM drive. The installation program starts, and the “IBM Director” window opens.

6. Click **Install IBM Director**. The “IBM Director Installation” window opens.
7. Click **IBM Director Agent installation**. The “IBM Director Agent Installation” window opens.
8. Click **32-bit installation**. The InstallShield wizard starts, and the “Welcome to the InstallShield Wizard” window opens.
9. Click **Next**. The “License Agreement” window opens.
10. Click **I accept the terms in the license agreement** and click **Next**. The “Feature and installation directory selection” window opens.

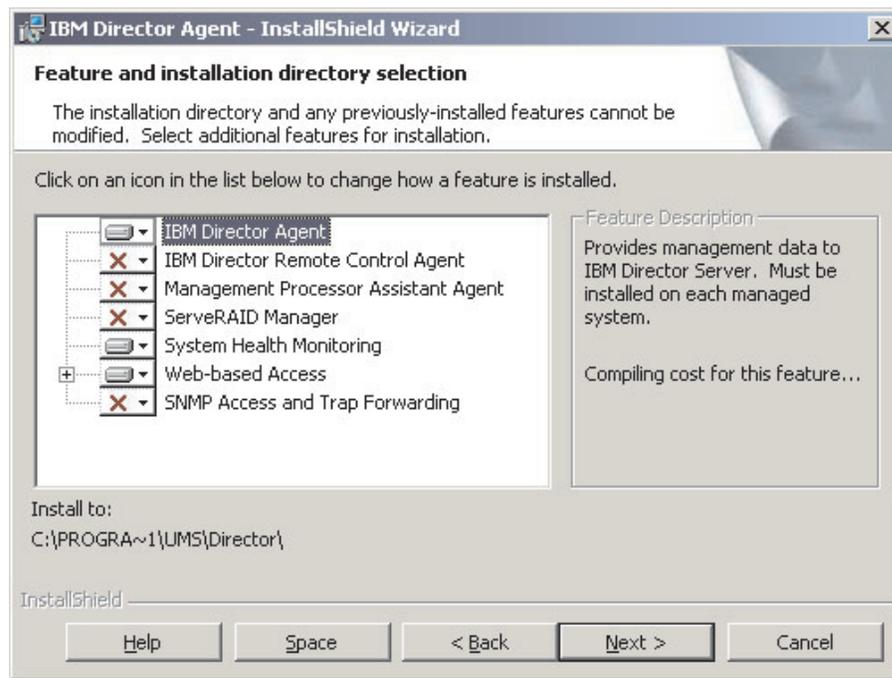


Figure 98. Upgrading IBM Director Agent on Windows: “Feature and installation directory selection” window

IBM Director Agent and any previously installed features are selected automatically for installation; a hard disk drive icon  is displayed to the left of the component.  is displayed to the left of uninstalled features.

11. If they were not installed previously, you can select to install the following features:

**IBM Director Remote Control Agent**

Enables a system administrator to perform remote desktop functions on the managed system

**Management Processor Assistant Agent**

Enables communication with service processors in IBM xSeries and Netfinity servers

**ServeRAID Manager**

Manages and monitors IBM ServeRAID adapters and integrated SCSI controllers with RAID capabilities

**System Health Monitoring**

Monitors the status of hardware components, produces and relays hardware alerts, and facilitates upward integration

**Web-based Access**

Enables system administrators to access the managed-system data through a Web browser or the Microsoft Management Console (MMC)

**SNMP Access and Trap Forwarding**

Enables access to managed-system data and alerts through SNMP

To select a feature, click  to the left of the feature name. A menu opens.

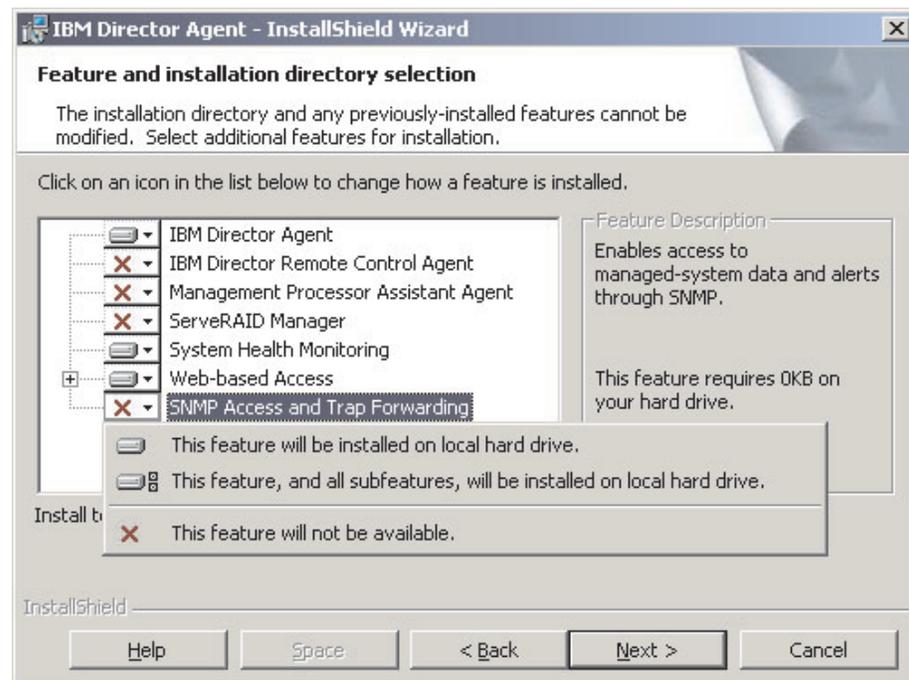


Figure 99. Upgrading IBM Director Agent on Windows: “Feature and installation directory selection” window

To install the feature, click either **This feature will be installed on local hard drive** or **This feature, and all subfeatures, will be installed on local hard drive**.

12. When you have selected the features that you want to install, click **Next**. The “Security settings” window opens.

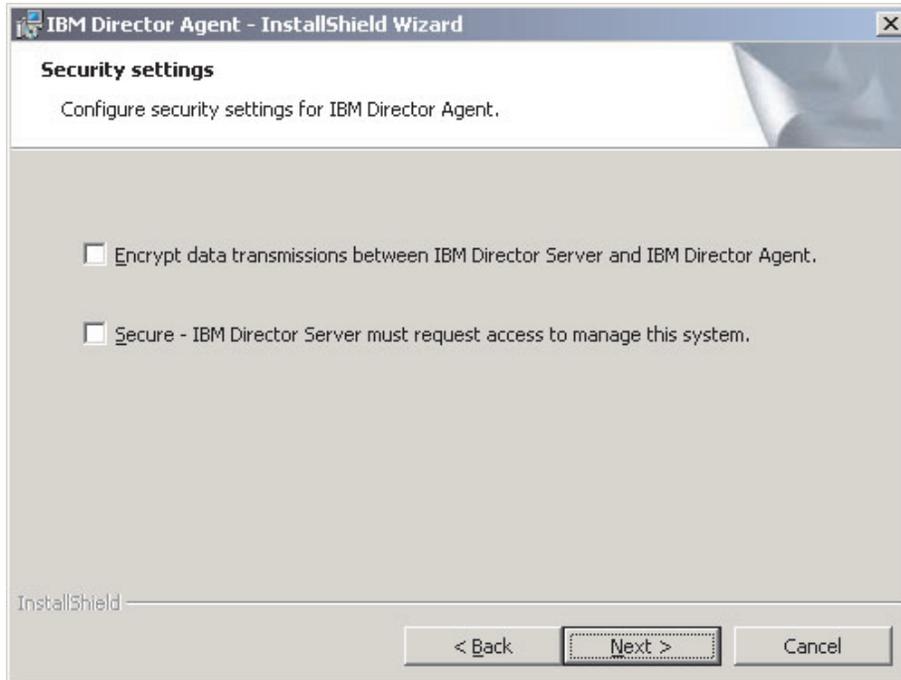


Figure 100. Upgrading IBM Director Agent on Windows: “Security settings” window

13. If you do not want to encrypt transmissions between IBM Director Server and IBM Director Agent, go to step 14. Otherwise, select the **Encrypt data transmissions between IBM Director Server and IBM Director Agent** check box.

**Note:** If encryption is enabled, the following conditions apply:

- The managed system is automatically secured, and the **Secure – IBM Director Server must request access to manage this system** check box is unavailable.
- Only management servers with encryption enabled are able to communicate with the managed system.

14. To set IBM Director Agent to the secured state, select the **Secure – IBM Director Server must request access to manage this system** check box. This ensures that only authorized instances of IBM Director Server can manage this system.
15. Click **Next**. The “Software Distribution settings” window opens.

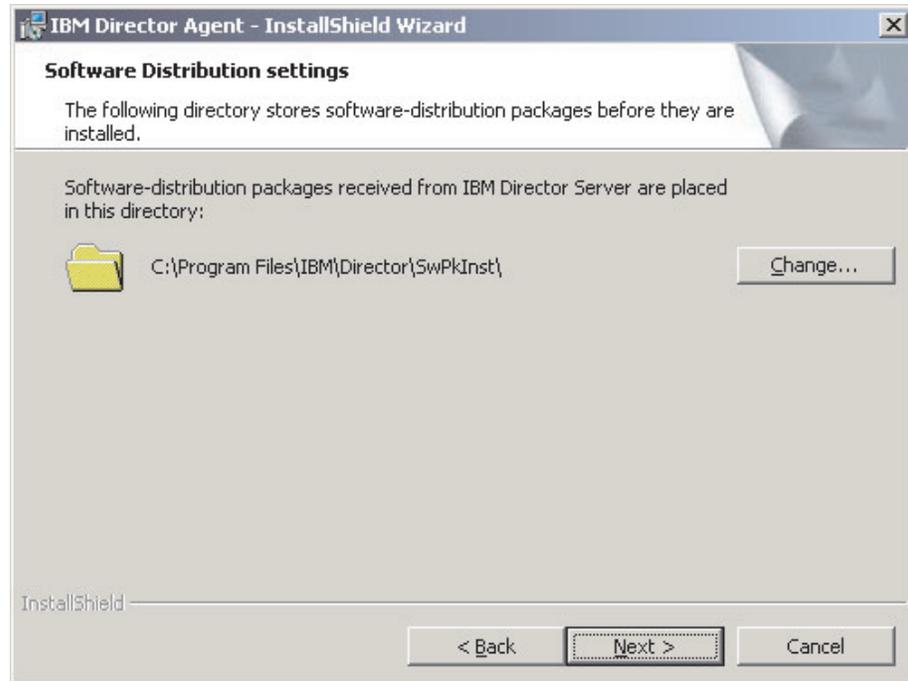


Figure 101. Upgrading IBM Director Agent on Windows: “Software Distribution settings” window

To select an alternative location where software-distribution packages are stored before being applied to IBM Director Agent, click **Change** and select another directory.

16. Click **Next**. If you did not select to install the Web-based Access feature, go to step 18 on page 180. Otherwise, the “Web-based Access information” window opens.

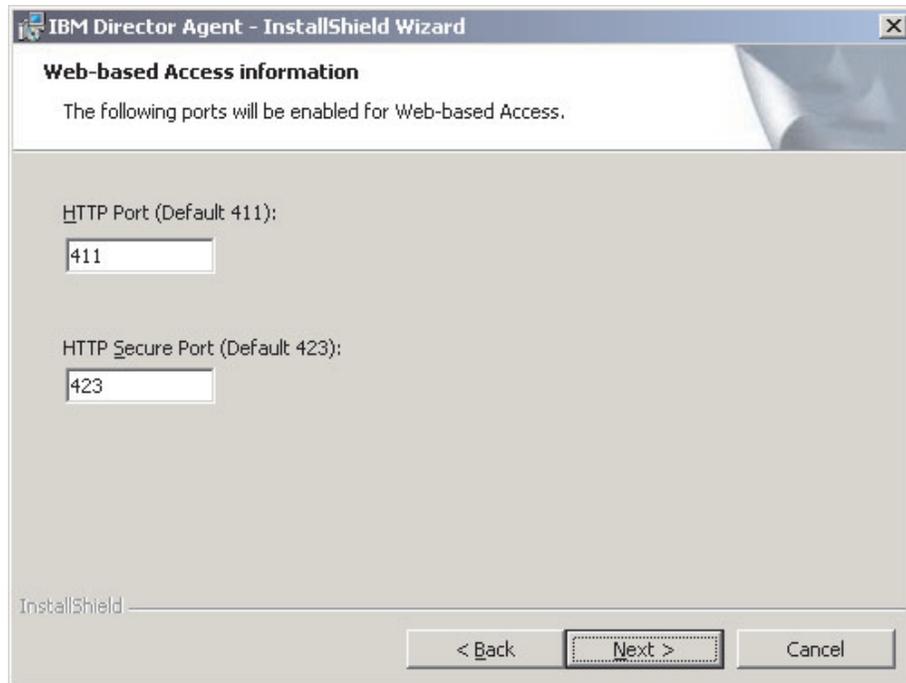


Figure 102. Upgrading IBM Director Agent on Windows: “Web-based Access information” window

17. Change the default HTTP port numbers (if necessary), and click **Next**. The “Ready to Install the Program window” opens.
18. Click **Install**. The “Installing IBM Director Agent” window opens. The status bar indicates the progress of the installation. When the installation is completed, the “Network driver configuration” window opens.

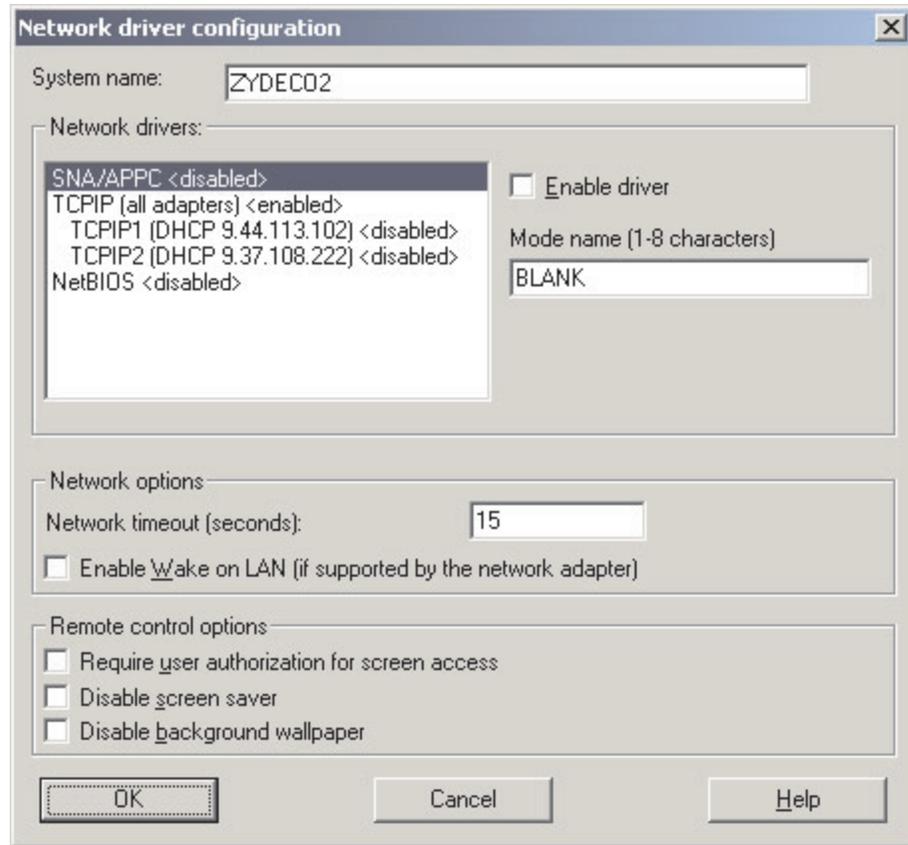


Figure 103. Upgrading IBM Director Agent on Windows: “Network driver configuration” window

19. In the **System Name** field, type the name that you want to be displayed in IBM Director Console. By default, this is the NetBIOS name of the managed system.
20. Define the communications protocols to use for communication between IBM Director Server and IBM Director Agent.
  - a. In the **Network drivers** field, TCPIP (all adapters) is enabled by default. To enable another protocol, select the protocol and then select the **Enable driver** check box.

**Note:** If you disable TCPIP (all adapters) and enable an individual device driver on a system with multiple network adapters, IBM Director Agent will receive *only* those data packets that are addressed to the individual adapter.

- b. In the **Network timeout** field, type the number of seconds that IBM Director Server waits for a response from IBM Director Agent. By default, this is set to 15 seconds.
- c. Select the **Enable Wake on LAN** check box if the network adapter supports the Wake on LAN feature.

**Note:** To determine whether your server supports the Wake on LAN feature, see your server documentation.

21. If you selected to install the IBM Director Remote Control Agent, the following options are available:

**Require User Authorization for System Access**

Select this check box to request authorization from the local user before accessing the managed system remotely.

**Disable Screen Saver**

Select this check box to disable the screen saver when the managed system is controlled remotely.

**Disable Background Wallpaper**

Select this check box to disable desktop wallpaper when the managed system is controlled remotely. You might want to disable the wallpaper because complicated backgrounds slow down remote control and increase network traffic.

22. Click **OK**. The status bar displays the progress of the installation. When the installation is completed, the “InstallShield Wizard Completed” window opens.
23. Click **Finish**. The “IBM Director Agent Installer” information window opens.
24. Remove the *IBM Director 4.20* CD from the CD-ROM drive.
25. Click **Yes** to restart your system.

For information about installing the IBM Director Server Plus Pack extensions, see Chapter 9, “Installing IBM Director extensions,” on page 131

## Performing an unattended upgrade of IBM Director Agent

You can perform an unattended upgrade of IBM Director Agent using a response file, which provides answers to the questions that are posed by the InstallShield wizard.

Complete the following steps to upgrade IBM Director Agent on Windows:

1. Stop IBM Director Agent. From a command prompt, type the following command and press Enter:  

```
net stop twgipc
```
2. Close all open applications.
3. Insert the *IBM Director 4.20* CD into the CD-ROM drive.
4. Copy the diragent.rsp file to a local directory. This file is in the director\agent\windows\i386 directory on the *IBM Director 4.20* CD.
5. From Windows Explorer, right-click the copy of the diragent.rsp file and then click **Properties**. The “diragent.rsp Properties” window opens. Clear the **Read-Only** check box and click **OK**.
6. Open the copy of the diragent.rsp file in an ASCII text editor.
7. Modify and save the diragent.rsp file. This file follows the Windows INI file format and is fully commented.

**Note:** Windows automatically detects and upgrades the IBM Director Agent features that were part of the existing IBM Director installation. However, you can select features that were not installed previously.

8. Change to the directory that contains the IBM Director Agent installation file (ibmsetup.exe). This file is in the director\agent\windows\i386 directory on the *IBM Director 4.20* CD.

9. From the command prompt, type the following command and press Enter:  
`ibmsetup.exe installationtype rsp="responsefile.rsp" waitforme`

where:

- *installationtype* is one of the following commands:
    - **unattended** shows the progress of the installation but does not require any user input.
    - **silent** suppresses all output to the screen during installation.
  - *responsefile.rsp* is the path and name of the response file that you created in step 7 on page 182.
  - **waitforme** is an optional parameter that ensures that `ibmsetup.exe` process will not end until the installation of IBM Director Agent is completed.
10. When prompted to do so, restart the operating system.
  11. Remove the *IBM Director 4.20* CD from the CD-ROM drive.

For information about installing the IBM Director Server Plus Pack extensions, see Chapter 9, “Installing IBM Director extensions,” on page 131.

## Upgrading IBM Director Agent on Windows (64-bit)

This section provides instructions for upgrading IBM Director Agent using the InstallShield wizard. The wizard can be used in a standard interactive mode, or you can perform an unattended installation using a response file to provide answers to the questions that the wizard poses.

When you upgrade IBM Director Agent, IBM Director automatically upgrades all previously installed IBM Director features. You also can choose to install additional features.

### Upgrading IBM Director Agent using the InstallShield wizard

Complete the following steps to upgrade IBM Director Agent on Windows:

1. Stop IBM Director Agent. From a command prompt, type the following command and press Enter:  
`net stop twgipc`
2. Close all applications, including any command-prompt sessions.
3. Insert the *IBM Director 4.20* CD into the CD-ROM drive.
4. If the installation program starts automatically and the InstallShield wizard starts, go to step 6 on page 176. Otherwise, click **Start** → **Run**.
5. In the **Open** field, type the following command and press Enter:  
`e:\setup.exe`

where *e* is the drive letter of the CD-ROM drive. The installation program starts, and the “IBM Director” window opens.

6. Click **Install IBM Director**. The “IBM Director Installation” window opens.
7. Click **IBM Director Agent installation**. The “IBM Director Agent Installation” window opens.
8. Click **64-bit installation**. The InstallShield wizard starts, and the “Welcome to the InstallShield Wizard” window opens.
9. Click **Next**. The “License Agreement” window opens.
10. Click **I accept the terms in the license agreement** and click **Next**. The “Feature and installation directory selection” window opens.

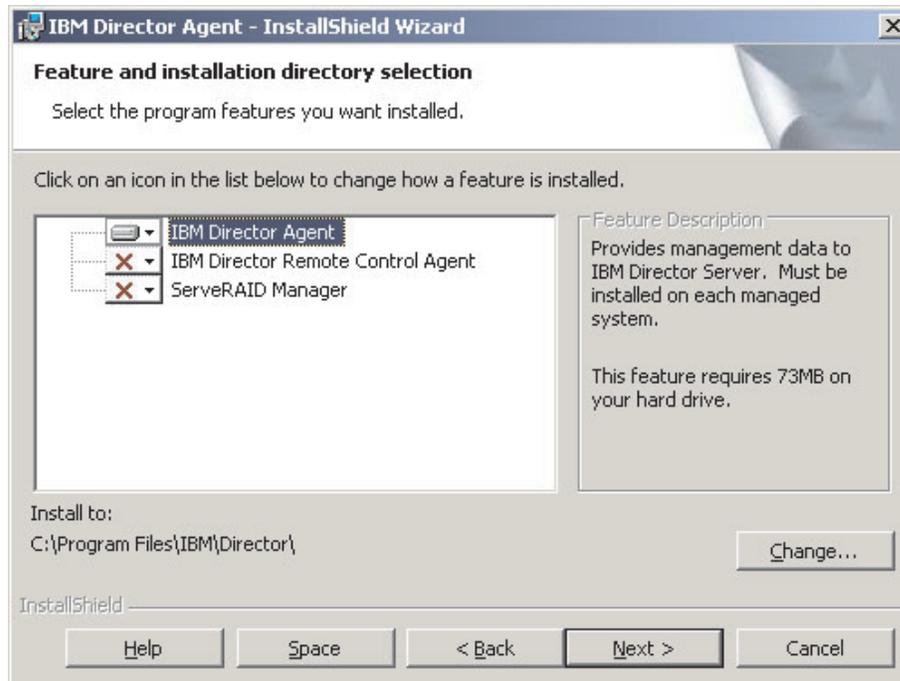


Figure 104. Installing IBM Director Agent on Windows: “Feature and installation directory selection” window

IBM Director Agent and any previously installed features are selected automatically for installation; a hard disk drive icon  is displayed to the left of the component.  is displayed to the left of uninstalled features.

11. If they were not installed previously, you can select to install the following features:

#### **IBM Director Remote Control Agent**

Enables a system administrator to perform remote desktop functions on the managed system

#### **ServeRAID Manager**

Manages and monitors IBM ServeRAID adapters and integrated SCSI controllers with RAID capabilities

To select a feature, click  to the left of the feature name. A menu opens. To install the feature, click either **This feature will be installed on local hard drive** or **This feature, and all subfeatures, will be installed on local hard drive**.

12. Click **Next**. The “Security settings” window opens.

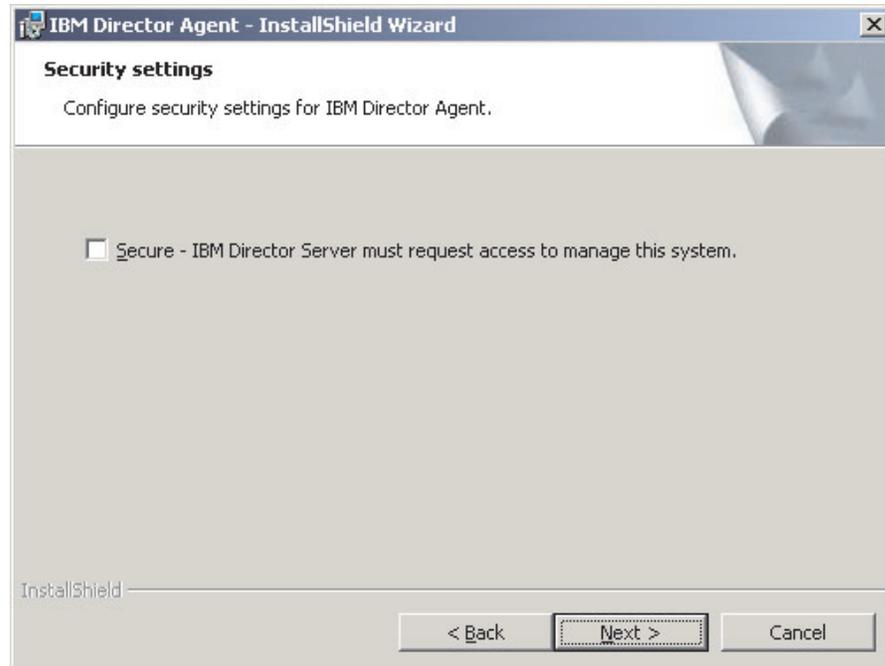


Figure 105. Installing IBM Director Agent on Windows: “Security settings” window

13. To set IBM Director Agent to the secured state, select the **Secure – IBM Director Server must request access to manage this system** check box. This ensures that only authorized instances of IBM Director Server can manage this system.
14. Click **Next**. The “Software Distribution settings” window opens.

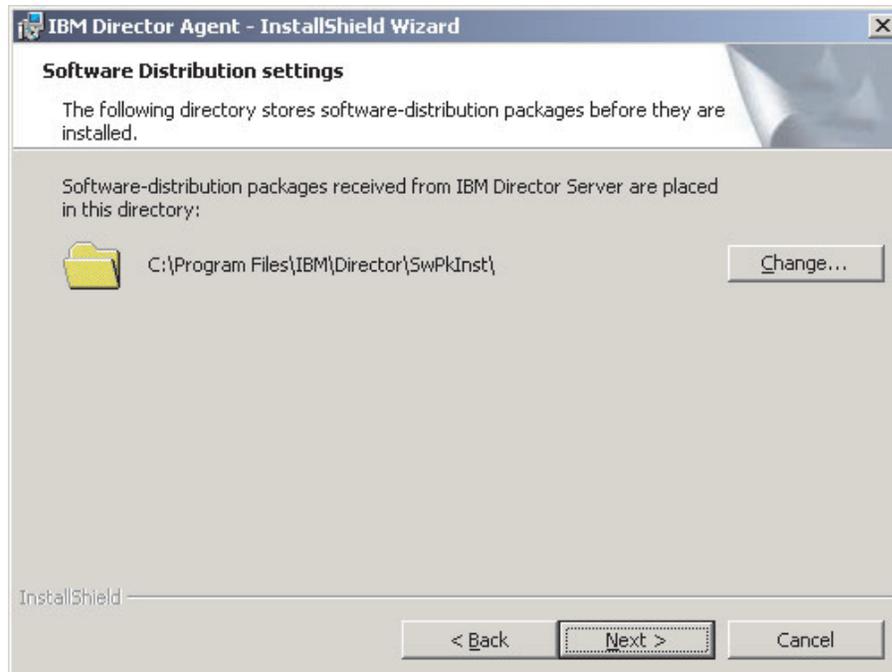


Figure 106. Upgrading IBM Director Agent on Windows: “Software Distribution settings” window

To select an alternative location where software-distribution packages are stored before being applied to IBM Director Agent, click **Change** and select another directory.

15. Click **Next**. The “Ready to Install the Program window” opens.
16. Click **Install**. The “Installing IBM Director Agent” window opens.  
The status bar indicates the progress of the installation. When the installation is completed, the “Network driver configuration” window opens.

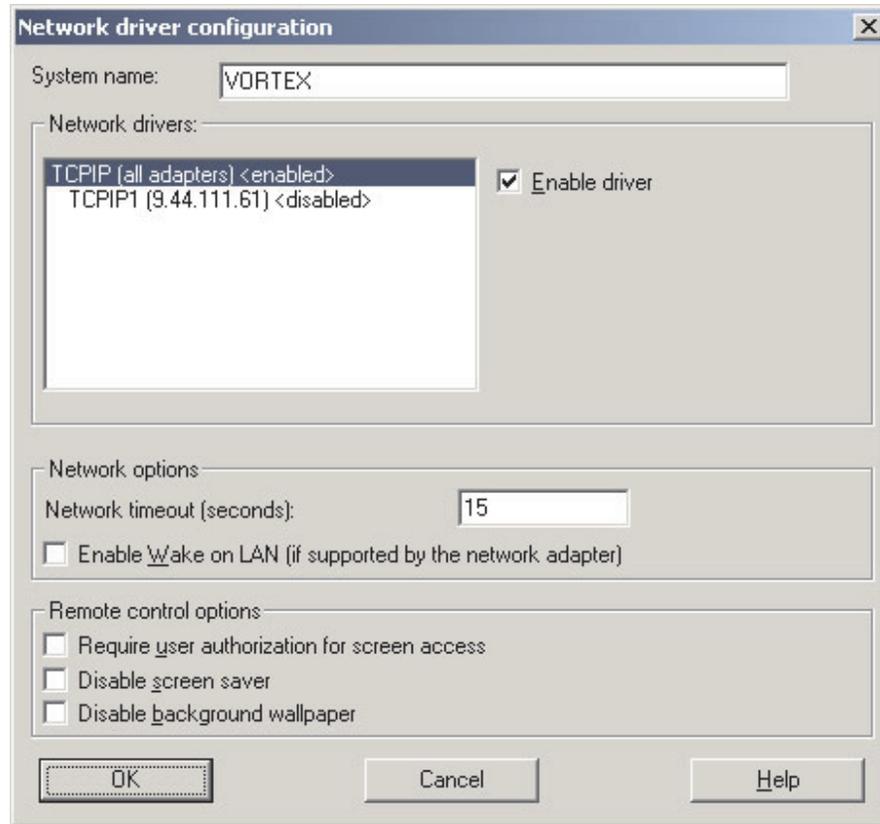


Figure 107. Installing IBM Director Agent on Windows: “Network driver configuration” window

17. In the **System Name** field, type the name that you want to be displayed in IBM Director Console. By default, this is the NetBIOS name of the managed system.
18. Define the communications protocols to use for communication between IBM Director Server and IBM Director Agent.
  - a. In the **Network drivers** field, TCPIP (all adapters) is enabled by default. To enable another protocol, select the protocol and then select the **Enable driver** check box.

**Note:** If you disable TCPIP (all adapters) and enable an individual device driver on a system with multiple network adapters, IBM Director Agent will receive *only* those data packets that are addressed to the individual adapter.

- b. In the **Network timeout** field, type the number of seconds that IBM Director Server waits for a response from IBM Director Agent. By default, this is set to 15 seconds.
- c. Select the **Enable Wake on LAN** check box if the network adapter supports the Wake on LAN feature.

**Note:** To determine whether your server supports the Wake on LAN feature, see your server documentation.

19. If you selected to install the IBM Director Remote Control Agent, the following options are available:

**Require User Authorization for System Access**

Select this check box to request authorization from the local user before accessing the managed system remotely.

**Disable Screen Saver**

Select this check box to disable the screen saver when the managed system is controlled remotely.

**Disable Background Wallpaper**

Select this check box to disable desktop wallpaper when the managed system is controlled remotely. You might want to disable the wallpaper because complicated backgrounds slow down remote control and increase network traffic.

20. Click **OK**. The status bar displays the progress of the installation. When the installation is completed, the “InstallShield Wizard Completed” window opens.
21. Click **Finish**. The “IBM Director Agent Installer” information window opens.
22. Remove the *IBM Director 4.20* CD from the CD-ROM drive.
23. Click **Yes** to restart your system.

## Performing an unattended upgrade of IBM Director Agent

You can perform an unattended upgrade of IBM Director Agent using a response file, which provides answers to the questions posed by the InstallShield wizard. You can use this method to create a standard installation file that can be used on many systems.

Complete the following steps to upgrade IBM Director Agent on Windows:

1. Stop IBM Director Agent. From a command prompt, type the following command and press Enter:  

```
net stop twgipc
```
2. Close all open applications.
3. Insert the *IBM Director 4.20* CD into the CD-ROM drive.
4. Copy the diragent.rsp file to a local directory. This file is in the director\agent\windows\ia64 directory on the *IBM Director 4.20* CD.
5. From Windows Explorer, right-click the copy of the diragent.rsp file and then click **Properties**. The “diragent.rsp Properties” window opens. Clear the **Read-Only** check box and click **OK**.
6. Open the copy of the diragent.rsp file in an ASCII text editor.
7. Modify and save the diragent.rsp file. This file follows the Windows INI file format and is fully commented.

**Note:** Windows automatically detects and upgrades the IBM Director Agent features that were part of the existing IBM Director installation. However, you can select features that were not installed previously.

8. Change to the directory that contains the IBM Director Agent installation file (ibmsetup.exe). This file is in the director\agent\windows\i386 directory on the *IBM Director 4.20* CD.

9. From the command prompt, type the following command and press Enter:  
`ibmsetup.exe installationtype rsp="responsefile.rsp" waitforme`

where:

- *installationtype* is one of the following commands:
    - **unattended** shows the progress of the installation but does not require any user input.
    - **silent** suppresses all output to the screen during installation.
  - *responsefile.rsp* is the path and name of the response file that you created in step 7 on page 182.
  - **waitforme** is an optional parameter that ensures that `ibmsetup.exe` process will not end until the installation of IBM Director Agent is completed.
10. If prompted to do so, restart the operating system.

**Note:** If you installed ServeRAID Manager for the first time, you must restart the managed system after the installation is completed. This ensures that the new features are detected.

11. Remove the *IBM Director 4.20* CD from the CD-ROM drive.

---

## Upgrading IBM Director Agent using the Software Distribution task

You can use the IBM Director Software Distribution task to upgrade IBM Director Agent on managed systems running Windows or Linux.

The following files describe IBM Director Agent, the LM78 device driver, and the IBM SMBus device driver:

- `diragent_linux.xml`
- `diragent_windows.xml`
- `diragent_windows64.xml`
- `lm78driver_linux.xml`
- `smbdriver_linux.xml`

You can download the files from the IBM Systems Management Software: Download/Electronic Support page at [http://www.ibm.com/pc/us/eserver/xseries/systems\\_management/dwnl.html](http://www.ibm.com/pc/us/eserver/xseries/systems_management/dwnl.html).

When you import the XML files into IBM Director, the Director Update Assistant creates software packages. Then, you can use the IBM Director Software Distribution task to distribute the packages to the managed systems.

To install the IBM LM78 or SMBus device driver using the Software Distribution task, you first must build the binary RPM file and copy it to the same directory as the `smbdriver_linux.xml` file. See “Downloading and installing the LM78 and SMBus device drivers” on page 170 for more information.

**Note:** If the IBM SMBus device driver for Linux, version 4.1, 4.11, or 4.12, is installed on the managed system, you must uninstall the device driver before installing the IBM SMBus device driver, version 4.20. See “Uninstalling an earlier version of the IBM SMBus device driver” on page 170 for more information.

## Creating a software package

Complete the following steps to create a software package:

1. Download the IBM Director Agent upgrade packages.
2. If you want to accept the default settings for the installation, go to step 3. Otherwise, open a copy of the `dirinstall` script or response file in an ASCII text editor. Modify the script or response file as needed; then, save the modified script or file.
3. Start IBM Director Console.
4. In the Tasks pane, double-click **Software Distribution**. The “Software Distribution Manager” window opens.



Figure 108. Creating a software package: “Software Distribution Manager” window (Standard Edition)



Figure 109. Creating a software package: “Software Distribution Manager” window (Premium Edition)

5. If you have not installed IBM Director 4.1 Software Distribution (Premium Edition), go to step 6. Otherwise, expand the **Wizards** tree.
6. Double-click **Director Update Assistant**. The “Director Update Assistant” window opens.

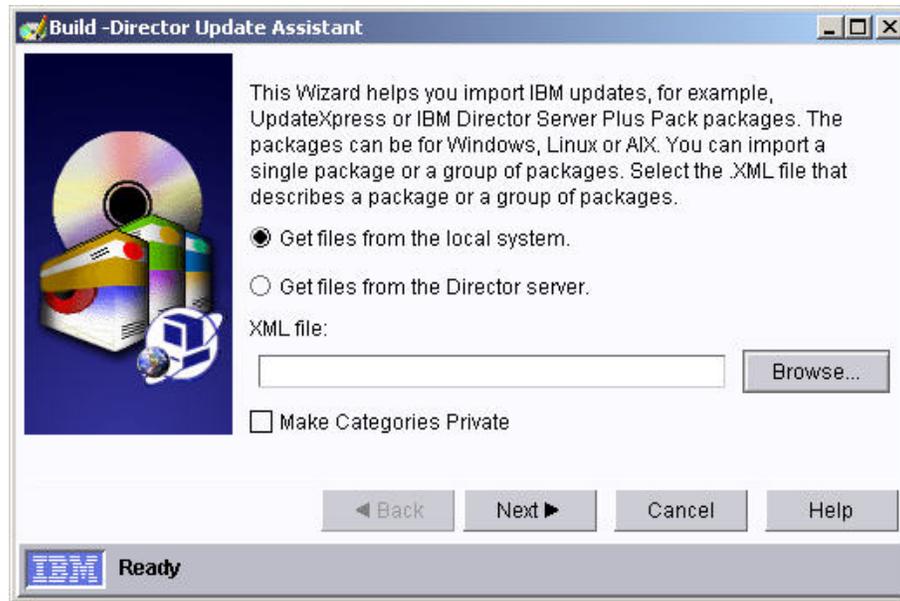


Figure 110. Creating a software package: “Director Update Assistant” window

7. If you want to get files from the management server, click **Get files from the Director server**. By default, **Get files from the local system** is selected.
8. To select a file, click **Browse**. The “IBM Update Package/Root Directory Location” window opens.

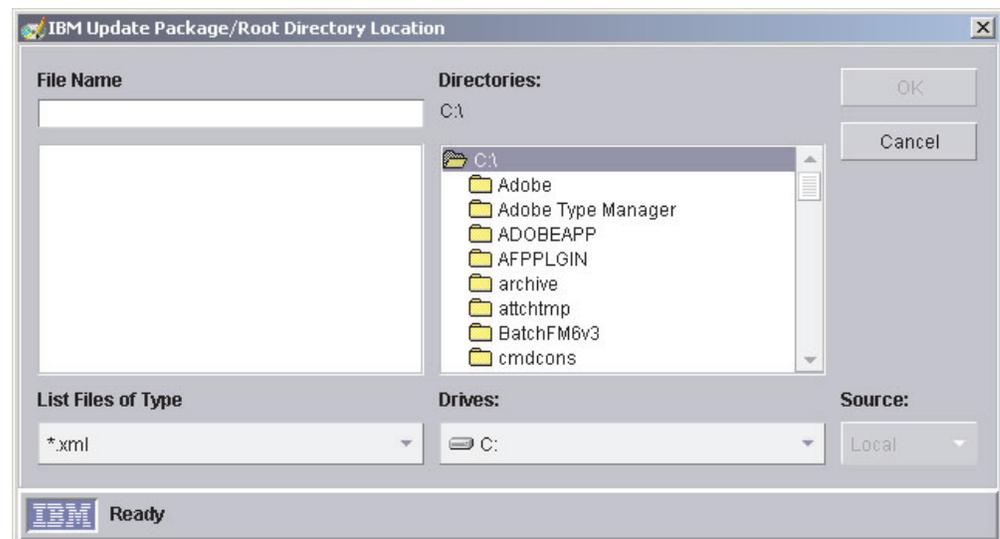


Figure 111. Creating a software package: “IBM Update Package/Root Directory Location” window

9. Locate the XML file and click it. The name of the XML file is displayed in the **File Name** field.

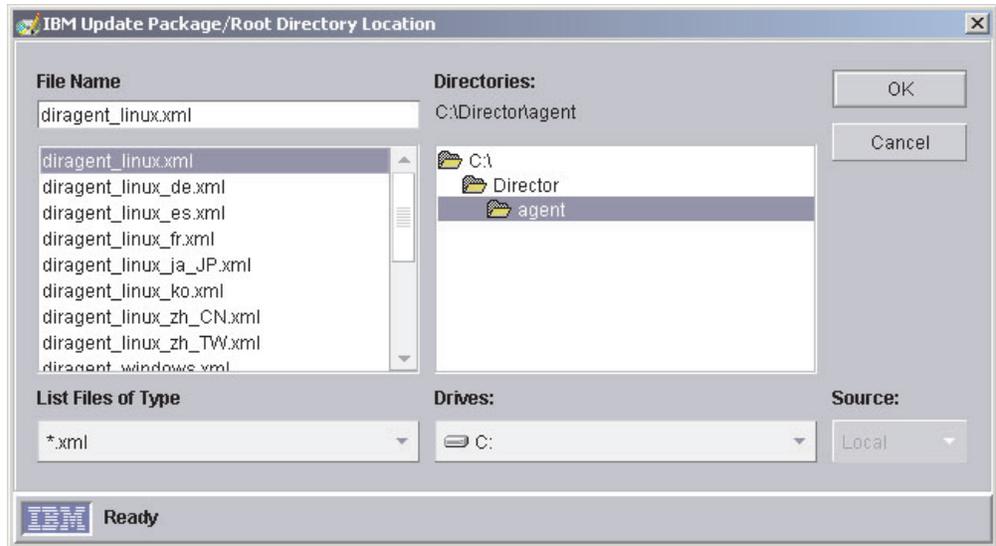


Figure 112. Creating a software package: “IBM Update Package/Root Directory Location” window

10. Click **OK**. The “Director Update Assistant” window reopens.



Figure 113. Creating a software package: “Director Update Assistant” window

11. Click **Next**. The second “Director Update Assistant” window opens.

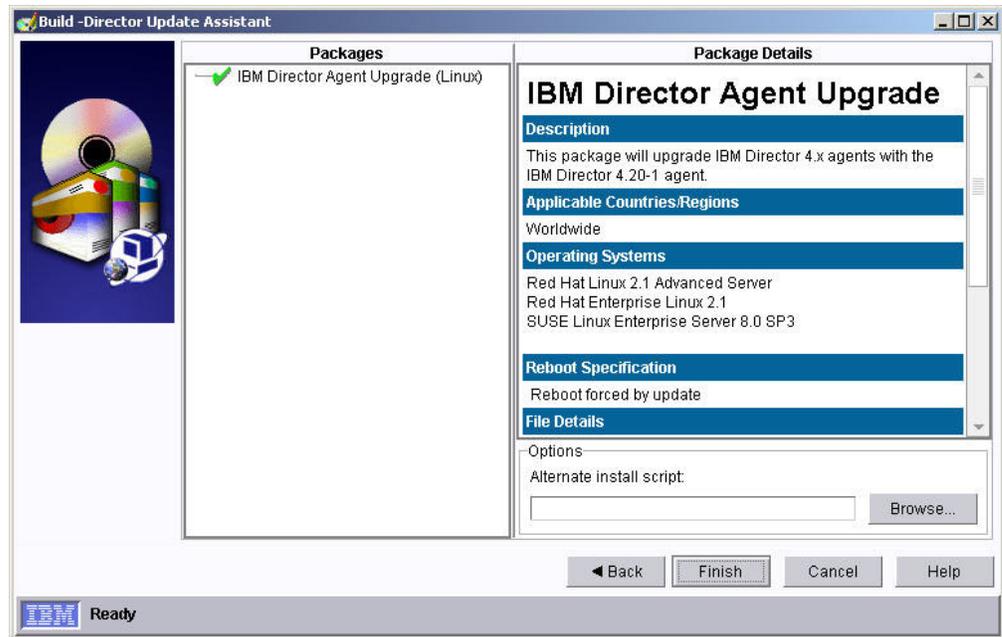


Figure 114. Creating software packages: “Director Update Assistant” window

12. To specify an alternative installation script or response file, click **Browse** and locate the file that you modified in step 2 on page 190.

**Note:** If you do not specify an alternative installation script or response file, IBM Director Agent is installed with the default settings that are specified in the diragent.rsp file or dirinstall script.

13. Click **Finish**. As the packages are processed, a status message is displayed at the bottom of the window.

When the processing is completed, the software-distribution packages are displayed in the Tasks pane of IBM Director Console.

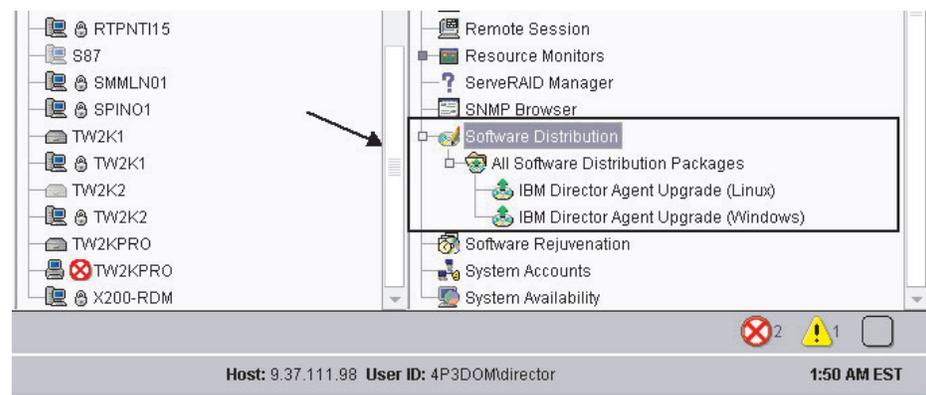


Figure 115. All Software Distribution Packages: IBM Director Agent Upgrade

## Installing a software package

Complete the following steps to install a software package:

1. Start IBM Director Console.
2. In the Tasks pane, expand the **Software Distribution** task.
3. Click the software package that you want to distribute. Then, drag it into the Group Contents pane and drop it onto the icon that is displayed for the system on which you want to install the software package. A window opens.

**Note:** To distribute software to several systems at once, you can drag the software package into the Groups pane and drop it onto the icon for the group. Alternatively, you can select multiple managed systems in the Group Contents pane.

4. When prompted Do you wish to create a scheduled job for this task or execute immediately?, click **Schedule** or **Execute Now**. If you click **Execute Now**, the software package is distributed immediately. If you click **Schedule**, the “New Scheduled Job” window opens.

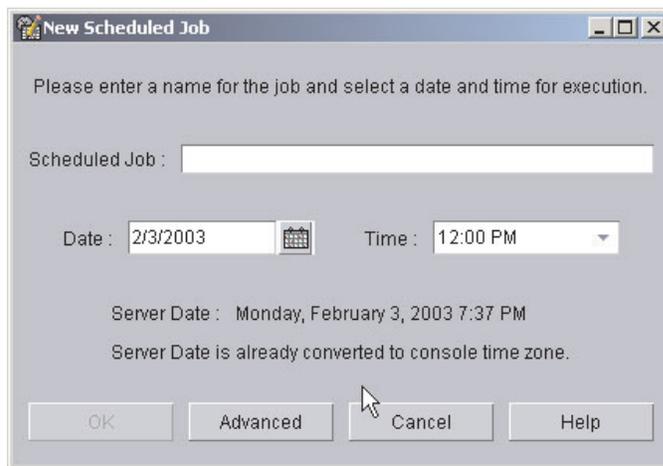


Figure 116. Scheduling the installation of a software package: “New Scheduled Job” window

5. Schedule the job:
  - a. In the **Scheduled Job** field, type a unique name for the job. This name is displayed in the Jobs pane of the Scheduler window.
  - b. In the **Date** field, type the day you want the software package to be installed (MM/DD/YYYY format).
  - c. In the **Time** field, type the time you want the software package to be installed.

For more information about the Scheduler task, see the *IBM Director 4.20 Systems Management Guide*.

6. Click **OK**. The “Save Job Confirmation” window opens.
7. Click **OK**.

---

## Part 5. Maintenance and problem solving



---

## Chapter 13. Modifying and uninstalling IBM Director

This chapter contains procedures for modifying and uninstalling IBM Director.

---

### Modifying an IBM Director installation

This section provides instructions for modifying an IBM Director installation on the following operating systems:

- AIX
- Linux
- NetWare
- Windows

You cannot use the Software Distribution task to modify an existing installation of IBM Director Agent.

### Modifying IBM Director running on AIX

After you install IBM Director Agent, you can enable the Wake on LAN feature. Complete the following steps to enable Wake on LAN for IBM Director Agent:

1. To stop IBM Director Agent, from a command prompt, type the following command and press Enter:  

```
/opt/ibm/director/bin/twgstop
```
2. Open an ASCII text editor and edit the ServiceNodeLocal.properties file. This file is in the /opt/ibm/director/data directory.
3. Modify the value of ipc.wakeonlan to read as follows:  

```
ipc.wakeonlan=1
```
4. Save and close the ServiceNodeLocal.properties file.
5. To start IBM Director Agent, type the following command and press Enter:  

```
/opt/ibm/director/bin/twgstart
```

### Modifying IBM Director running on Linux

After you install IBM Director, you can modify the installation. You can configure the IBM Director database, enable Wake on LAN for IBM Director Agent, install a previously uninstalled feature, or remove a feature.

**Note:** Before you configure a database for use with IBM Director, make sure that you have completed any necessary preinstallation tasks. See “Preparing the IBM Director database” on page 28 for more information.

#### Installing the database after IBM Director Server is installed

Complete the following steps to install and configure a database after you have installed IBM Director Server:

1. To stop IBM Director Server, from a command prompt, type the following command and press Enter:  

```
/opt/IBM/director/bin/twgstop
```
2. Type the following command and press Enter:  

```
/opt/IBM/director/bin/cfgdb
```

3. Follow the instructions on the screen.
4. To restart IBM Director Server, type following command and press Enter:  
`/opt/IBM/director/bin/twgstart`

### Enabling the Wake on LAN feature

Complete the following steps to enable Wake on LAN for IBM Director Agent:

1. To stop IBM Director Agent, from a command prompt, type the following command and press Enter:

```
/opt/Variable/director/bin/twgstop
```

where *Variable* is one of the following strings:

<b>For 32-bit operating systems or operating systems for AMD64</b>	IBM
<b>For operating systems for Intel Itanium or IBM iSeries and IBM pSeries</b>	ibm

2. Open an ASCII text editor and edit the ServiceNodeLocal.properties file. This file is in either the `/opt/IBM/director/data` or `/opt/ibm/director/data` directory.
3. Modify the value of `ipc.wakeonlan` to read as follows:  
`ipc.wakeonlan=1`
4. Save and close the ServiceNodeLocal.properties file.
5. To start IBM Director Agent, type the following command and press Enter:

```
/opt/Variable/director/bin/twgstart
```

where *Variable* is one of the following strings:

<b>For 32-bit operating systems or operating systems for AMD64</b>	IBM
<b>For operating systems for Intel Itanium or IBM iSeries and IBM pSeries</b>	ibm

### Enabling SNMP Access and Trap Forwarding for Linux

Complete the following steps to enable SNMP Access and Trap Forwarding for managed systems running Linux:

1. Download Net-SNMP, version 5.0.9 from the Net-SNMP Web site at <http://www.net-snmp.org/>. You will need one of the following files:

<b>For Red Hat Linux, version 2.1</b>	net-snmp-5.0.9-4.rh73.i386.rpm
<b>For Red Hat Linux, version 3.0</b>	net-snmp-5.0.9-4.rh9.i386.rpm
<b>For SUSE LINUX Enterprise Server 8 for x86</b>	net-snmp-5.0.9.tar.gz

**Note:** Net-SNMP is not supported on VMware console operating systems.

2. Install Net-SNMP
3. Use the **snmpconf** utility to configure Net-SNMP for access groups and trap destinations. If you installed the precompiled binary files for Red Hat Linux, the `snmpconf` utility is in the `/user/bin` directory.

- Open the `snmpd.conf` file in an ASCII text editor and locate the following section:

```
# master: Should the agent operate as a master agent or not.
# Currently, the only supported master agent type for this token
# is "agentx".
#
# arguments: (on|yes|agentx|all|off|no)
master agentx
```

If you installed the precompiled binary files for Red Hat Linux, the `snmpd.conf` file is located in the `/usr/local/share/snmp` directory.

- Make sure that the line that contains the `master agentx` string is uncommented. If necessary, remove the hash (`#`) at the beginning of the line. Save the modified file.
- If the Net-SNMP installation did not install the Net-SNMP libraries into a system library path, you must modify the `dacimom` and `dirsnmpd` startup scripts. Locate these scripts. They are installed with IBM Director Agent and are located in the following directories:

<b>For Red Hat Linux</b>	<code>/etc/rc.d/init.d</code>
<b>For SUSE LINUX</b>	<code>/etc/init.d</code>

- Open the `dacimom` script and add the following line:
 

```
export LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:/usr/local/lib
```
- Locate the following line in the `dirsnmpd` script:
 

```
export LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:/${CIMOM_ROOTDIR}/lib
```
- Add `:/usr/local/lib` to the end of the line, so that the line reads as follows (all on one line):
 

```
export LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:/${CIMOM_ROOTDIR}/lib:/usr/local/lib
```

### Installing an IBM Director feature

Complete the following steps to add a previously uninstalled feature to IBM Director Server, IBM Director Console, and IBM Director Agent:

- Make a copy of the applicable `dirinstall` script. This file is in one of the following directories on the applicable *IBM Director 4.20* CD:

<b>For 32-bit operating systems</b>	<code>/director/component/linux/i386</code>
<b>For operating systems for AMD64</b>	<code>/director/agent/linux/i386</code>
<b>For operating systems for Intel Itanium</b>	<code>/director/agent/linux/ia64</code>
<b>For operating systems for IBM pSeries and IBM iSeries</b>	<code>/director/agent/linux/ppc</code>

where *component* is `server`, `console`, or `agent`.

- Open an ASCII text editor and modify the "User configuration" section of the `dirinstall` script.
- Save the modified installation script.

- To stop IBM Director Agent, from a command prompt, type the following command and press Enter:

```
/opt/Variable/director/bin/twgstop
```

where *Variable* is one of the following strings:

<b>For 32-bit operating systems or operating systems for AMD64</b>	IBM
<b>For operating systems for Intel Itanium or IBM iSeries and IBM pSeries</b>	ibm

- Run the dirinstall script. Type the following command and press Enter:

```
/SourceDirectory/dirinstall
```

where *SourceDirectory* is the directory to which you copied the modified installation script

- To start IBM Director Agent, type the following command and press Enter:

```
/opt/Variable/director/bin/twgstart
```

where *Variable* is one of the following strings:

<b>For 32-bit operating systems or operating systems for AMD64</b>	IBM
<b>For operating systems for Intel Itanium or IBM iSeries and IBM pSeries</b>	ibm

You also can use the standard RPM commands.

## Uninstalling an IBM Director feature

Complete the following steps to remove a feature from IBM Director Server, IBM Director Console, and IBM Director Agent:

- Modify the diruninstall script, which is in either the IBM/director/bin or ibm/director/bin directory. By default, this script removes all detected IBM Director components.
- Save the modified uninstallation script.
- To stop IBM Director Agent, from a command prompt, type the following command and press Enter:

```
/opt/Variable/director/bin/twgstop
```

where *Variable* is one of the following strings:

<b>For 32-bit operating systems or operating systems for AMD64</b>	IBM
<b>For operating systems for Intel Itanium or IBM iSeries and IBM pSeries</b>	ibm

- Run the diruninstall script. Type the following command and press Enter:

```
/SourceDirectory/diruninstall
```

where *SourceDirectory* is the directory to which you copied the modified uninstallation script.

5. To start IBM Director Agent, type the following command and press Enter:

```
/opt/Variable/director/bin/twgstart
```

where *Variable* is one of the following strings:

<b>For 32-bit operating systems or operating systems for AMD64</b>	IBM
<b>For operating systems for Intel Itanium or IBM iSeries and IBM pSeries</b>	ibm

You also can use the standard RPM commands.

**Note:** (KDE environment only) If you plan to use kpackage, make sure that the **Use scripts** check box is cleared.

## Modifying IBM Director running on NetWare

### Notes:

1. You cannot use this procedure to uninstall ServeRAID Manager or the MPA Agent. However, you can use this procedure to add either component to an existing IBM Director Agent installation.
2. To modify an IBM Director Agent installation, you must log on to the NetWare server from a Windows workstation running the NetWare Client for Windows.
3. The SYS volume must be mapped as a drive to the system running Windows.
4. You must have administrator or supervisor access on the NetWare server.

Complete the following steps to add a previously uninstalled feature to IBM Director Agent:

1. Stop IBM Director Agent. From the server running NetWare, change to the console screen. Type the following command and press Enter:  

```
unload twgipc
```
2. Insert the *IBM Director 4.20* CD into the CD-ROM drive of the system running Windows. If the autorun window opens, close it.
3. Start Windows Explorer, and open the `\director\agent\netware` directory.
4. Double-click **setup.exe**. The InstallShield wizard starts.
5. Click **Next**. The “Installing IBM Director Agent” window opens.
6. Click **Next** to accept the license agreement. The “Choose destination location” window opens.

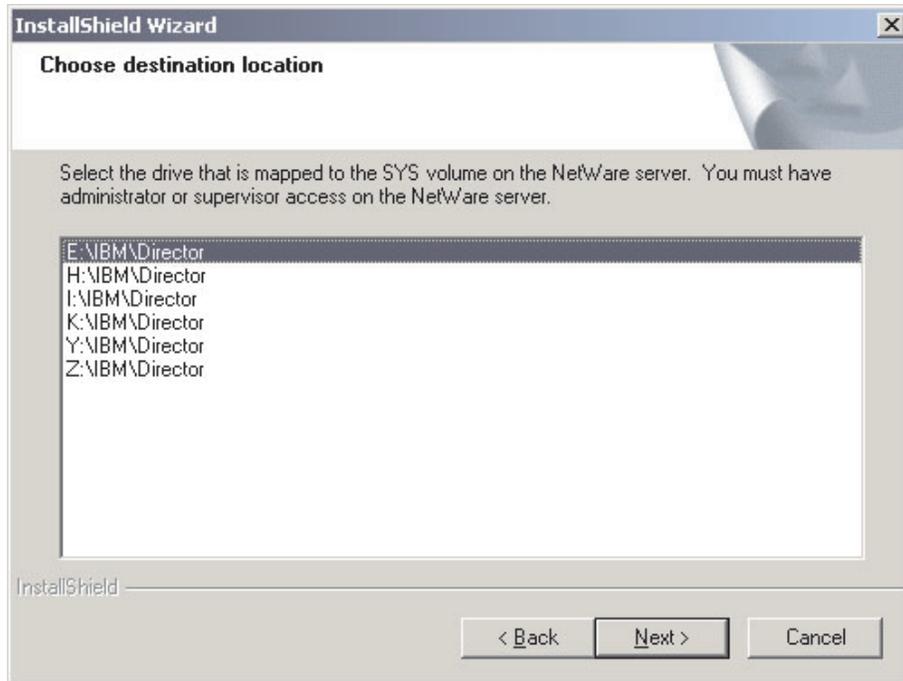


Figure 117. Modifying IBM Director Agent on NetWare: “Choose destination location” window

7. Click the drive that is mapped to the SYS volume on the NetWare server; then, click **Next**. The “Select Components” window opens.

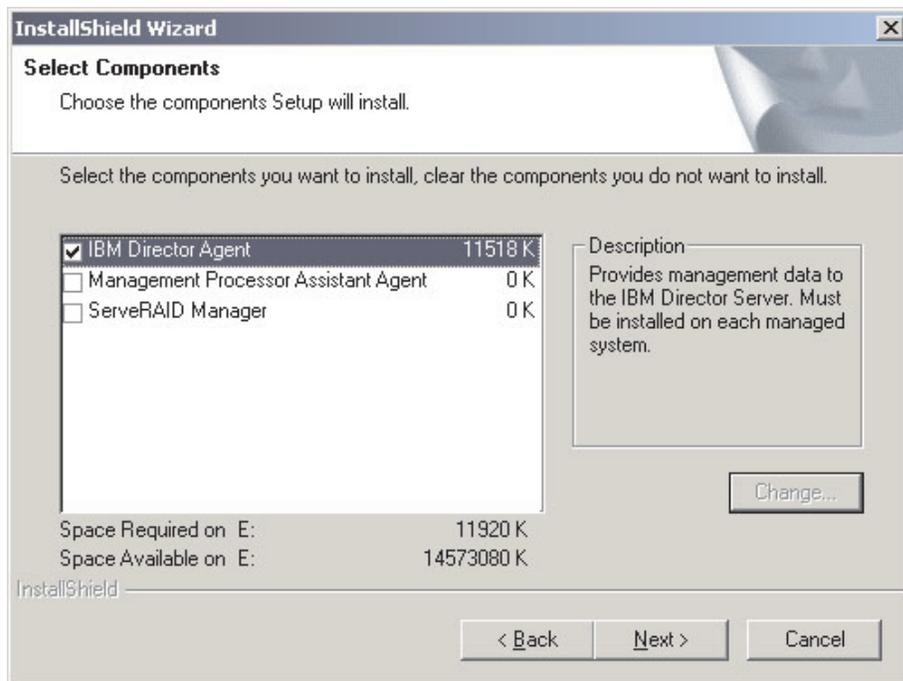


Figure 118. Modifying IBM Director Agent on NetWare: “Select Components” window

8. Select the check boxes for the components that you want to add.

9. Click **Next**. The Setup Status window opens, and the IBM Director Agent installation begins. When the installation is completed, the “InstallShield Wizard Complete” window opens.
10. Click **Finish**.
11. On the NetWare server, change to the console screen.
12. Type the following command and press Enter:

```
load twgipc
```

## Modifying IBM Director running on Windows

After you install IBM Director, you can modify the installation. You can configure the IBM Director database, install a previously uninstalled feature, or remove a feature.

### Notes:

1. Before you configure a database for use with IBM Director, make sure that you have completed any necessary preinstallation tasks. See “Selecting the IBM Director database application” on page 22 and “Preparing the IBM Director database” on page 28.
2. If both System Health Monitoring and MPA Agent are installed, you cannot remove System Health Monitoring only. To remove System Health Monitoring, you first must uninstall MPA Agent. When the uninstallation process is completed, uninstall System Health Monitoring.

### Configuring the database after IBM Director Server is installed

Complete the following steps to configure a database after you have installed IBM Director Server:

1. Stop IBM Director Server. From a command prompt, type the following command and press Enter:

```
net stop twgipc
```

2. Type the following command and press Enter:

```
cfgdb
```

The “IBM Director database configuration” window opens.

3. Follow the instructions on the screen. For more information, see “Installing IBM Director Server on Windows” on page 44. Steps 25 through 32 detail the process of selecting and configuring a database for use with IBM Director Server.

### Installing or uninstalling an IBM Director feature

Complete the following steps to add a previously uninstalled feature to or remove a feature from IBM Director Server, IBM Director Console, or IBM Director Agent:

1. Click **Start** → **Settings** → **Control Panel**. The “Control Panel” window opens.
2. Double-click **Add/Remove Programs**. The “Add/Remove Programs” window opens.
3. Click the IBM Director software component that you want to modify; then, click **Change**. The InstallShield wizard starts, and the “Welcome to the InstallShield Wizard” window opens.
4. Click **Next**. The “Program Maintenance” window opens.

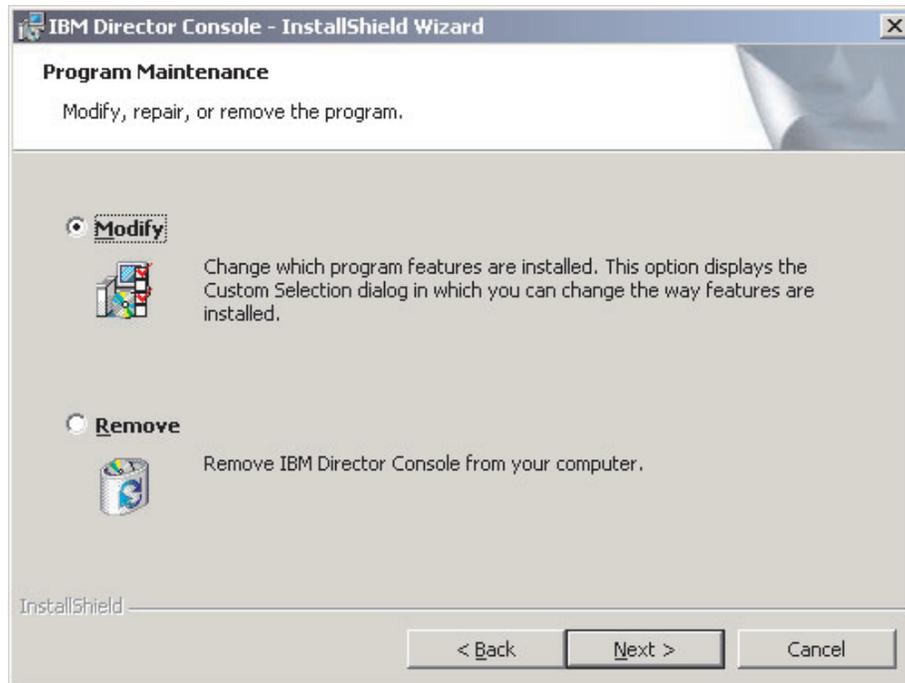


Figure 119. “Program Maintenance” window

5. Click **Modify**; then, click **Next**.
6. Continue through the wizard, making changes as necessary. For more information, see “Installing IBM Director Server on Windows” on page 44, “Installing IBM Director Console on Windows” on page 58, “Installing IBM Director Agent on Windows (32-bit)” on page 71, or “Installing IBM Director Agent on Windows (64-bit)” on page 78.

If you modify an IBM Director Agent installation by adding either ServeRAID Manager or MPA Agent, be sure to restart the managed system after the installation is completed. This ensures that the new components are detected.

You also can remove Server Plus Pack extensions by issuing the **dirunins** command from a command-line prompt. See “Uninstalling IBM Director using the dirunins command” on page 207 for more information.

---

## Uninstalling IBM Director

You can use the following procedures to uninstall IBM Director.

**Note:** You can retain the configuration data when you uninstall IBM Director. This enables you to reinstall IBM Director and access the saved configuration data. Be sure to reinstall IBM Director in the same location.

## Uninstalling IBM Director Agent on AIX

To uninstall IBM Director Agent, type the following command and press Enter:

```
installp -u IBM.Director.Agent.IBMDirA
```

## Uninstalling IBM Director on i5/OS

This section contains instructions for uninstalling IBM Director Server and IBM Director Agent running on i5/OS.

### Uninstalling IBM Director Server on i5/OS

**Note:** To uninstall IBM Director Server, you must connect to the server running i5/OS from a system running Windows. The system running Windows must have JRE, version 1.3.1 or later, installed.

Complete the following steps to uninstall IBM Director Server running on i5/OS:

1. If necessary, map the integrated file system (IFS) root directory on the i5/OS server as a drive to the system running Windows.
2. From a command prompt, type the following command (all on one line) and press Enter:

```
java -jar Q:\QIBM\ProdData\VE\Director\_uninst\uninstall.jar -os400  
-silent
```

where **-silent** is an optional parameter that specifies that the uninstallation occurs in unattended mode.

3. (Optional) Delete the following directories:

- `q:\QIBM\UserData\Director`
- `q:\QIBM\ProdData\VE\Director\_uninst`

where *q* is the drive letter of the drive that you mapped in step 1.

### Uninstalling IBM Director Agent on i5/OS

Complete the following steps to uninstall IBM Director Agent running on i5/OS:

1. If necessary, map the IFS root directory on the i5/OS server as a drive to the system running Windows.
2. Use the following OS/400 Delete Licensed Programs (DLTLICPGM) command to uninstall IBM Director Agent:

```
DLTLICPGM LICPGM(5733VE1) OPTION(39)
```

3. (Optional) Delete the `q:\QIBM\UserData\Director` directory, where *q* is the drive letter of the drive that you mapped in step 1.

## Uninstalling IBM Director on Linux

Use the `diruninstall` script, which is in the `IBM/director/bin` directory. This script removes all IBM Director components, including the Server Plus Pack extensions. To uninstall IBM Director, type the following command and press Enter:

```
/opt/variable/director/bin/diruninstall
```

where *variable* is one of the following strings:

<b>For 32-bit operating systems or operating systems for AMD64</b>	IBM
<b>For operating systems for Intel Itanium or IBM iSeries and IBM pSeries</b>	ibm

You also can use standard RPM commands. Consider the following information:

- You must uninstall MPA, ServeRAID Manager, and any IBM Director extensions *before* uninstalling IBM Director Server, IBM Director Console, or IBM Director Agent.
- If an IBM Director database is configured, you must delete the tables and remove the IBM Director database configuration. Perform this task *after* all other packages are removed but *before* uninstalling IBM Director Server. From a command prompt, type the following command and press Enter:

```
/opt/IBM/director/bin/uncfgdb
```

When you uninstall packages on Linux, the following files are retained to make it possible to restore persistent data:

- /opt/IBM/director.save.1/saveddata.tar
- /etc/TWGagent/TWGagent.uid

## Uninstalling IBM Director Agent on NetWare

Complete the following steps to uninstall IBM Director Agent on NetWare:

1. From the server running NetWare, change to the console screen.
2. Type the following command and press Enter:

```
unload twgipc
```
3. Using an ASCII text editor, open the autoexec.ncf file and remove the following lines:

```
:*****IBM Director Agent*****  
Search add sys:IBM\Director  
load twgipc  
:*****IBM Director agent*****
```
4. Save the modified autoexec.ncf file.
5. Shut down and restart the server running NetWare.
6. From a Windows workstation running the NetWare Client for Windows, map a drive to the SYS volume and delete the IBM\Director directory.

## Uninstalling IBM Director on Windows

You can uninstall IBM Director either by using the Windows Add/Remove Programs feature or from a command-line prompt.

### Uninstalling IBM Director using the Windows Add/Remove Programs feature

Complete the following steps to uninstall IBM Director:

1. Shut down all applications.
2. Click **Start** → **Settings** → **Control Panel**. The “Control Panel” window opens.
3. Double-click **Add/Remove Programs**. The “Add/Remove Programs” window opens.
4. Click the IBM Director software component that you want to remove; then, click **Remove**.
5. Follow the instructions on the screen.

## Uninstalling IBM Director using the `dirunins` command

From a command-line prompt, type the following command and press Enter:

```
dirunins option directorcomponent
```

The following table contains information about the possible values for *option* and *directorcomponent*.

Table 26. *dirunins* parameters

Variable	Parameter	What it does
<i>option</i>	<code>debug</code>	Logs all messages that are sent by the Windows Installer log engine, including status and information messages
	<code>deletedata</code>	Deletes all configuration data
	<i>logfile</i>	Specifies the fully qualified name of an alternative installation log file
	<code>noreboot</code>	Suppresses any required restart
	<code>silent</code>	Suppresses all output to the screen
	<code>unattended</code>	Shows the progress of the uninstallation but does not require any user input
	<code>verbose</code>	Enables verbose logging
<i>directorcomponent</i>	<code>server</code>	Uninstalls IBM Director Server and any installed Server Plus Pack extensions
	<code>console</code>	Uninstalls IBM Director Console and any installed Server Plus Pack extensions
	<code>agent</code>	Uninstalls IBM Director Agent
	<code>capmgt</code>	Uninstalls Capacity Manager
	<code>swrejuv</code>	Uninstalls Software Rejuvenation
	<code>sysavail</code>	Uninstalls System Availability
	<code>activepci</code>	Uninstalls Active PCI Manager

**Note:** If you are uninstalling IBM Director Agent, be sure to uninstall any installed Server Plus Pack extensions before uninstalling IBM Director Agent.



---

## Chapter 14. Solving IBM Director problems

This chapter describes some of the problem symptoms and suggested solutions for the following procedures, components, and features in IBM Director 4.20:

- Installation, upgrades, and uninstallation (see page 209)
- IBM Director Server (see page 211)
- IBM Director Console (see page 215)
- IBM Director Agent (see page 219)
- Managed systems running Windows (see page 220)
- IBM Director tasks (see page 221)
- Software Distribution (see page 224)
- Web-based Access (see page 226)
- Systems running double-byte character set (DBCS) languages (see page 227)

---

### Installation, upgrades, and uninstallation

This section describes problems that might occur when you install, upgrade, or uninstall IBM Director.

#### Installation

Table 27 describes problems that might occur when you install IBM Director.

Table 27. Installation problems

Symptom	Suggested action
(Windows only) When you install IBM Director, the following message is displayed: Error 1722. There is a problem with this Windows Installer package. A program run as part of the setup did not finish as expected. Contact your support personnel or package vendor.	The monitor for a system running IBM Director Server or IBM Director Console must support at least 256 colors. Increase the display color palette to more than 256 colors, uninstall the partial installation, and reinstall IBM Director Server.
(Windows only) When an installation of IBM Director Agent is canceled, files are left in directories.	Delete the following files: <ul style="list-style-type: none"><li>• <i>designated_drive</i>\IBM\Director\data</li><li>• <i>designated_drive</i>\IBM\Director\data\map</li><li>• <i>designated_drive</i>\IBM\Director\data\script</li><li>• <i>designated_drive</i>\IBM\Director\data\snmp</li></ul> where <i>designated_drive</i> is the directory that you designated for the installation.
(Windows only) When you modify IBM Director Agent or IBM Director Console, you are prompted for the location of either the IBM Director Agent.msi file or the IBM Director Console.msi file.	Extract the files from the Web installation package that you used when you installed IBM Director Agent or IBM Director Console. When prompted for the location of the IBM Director Agent.msi file or the IBM Director Console.msi file, specify the directory where the extracted files are located.
(Windows Server 2003 only) When IBM Director Server or IBM Director Agent starts for the first time on an ASF-capable system, the event log might contain traps or exceptions.	IBM Director Server or IBM Director Agent completed installation before the system management bus (SMBus) was detected and the device driver installed.  When you install IBM Director Server or IBM Director Agent, be sure that the SMBus device driver is installed before you restart the system.

Table 27. Installation problems (continued)

Symptom	Suggested action
(Windows Server 2003 only) During installation of IBM Director Agent, Windows might display the following blue screen trap: IRQL_NOT_LESS_OR_EQUAL	This problem is solved by a Microsoft update. See the Microsoft Knowledge Base Article 825236 for more information.

## Upgrades

Table 28 describes problems that might occur when you upgrade IBM Director.

Table 28. Upgrade problems

Symptom	Suggested action
Error message 1306 is displayed.	Modify the settings for the IBM Director Support Program Service (TWGIPC). If Web-based Access is installed, you also must modify the settings for the IBM Director Agent Web Server (DirWbs). For both services, set the startup type to <b>Manual</b> . Restart (reboot) the management server, and then begin the uninstallation again.
When you upgrade from IBM Director 3.1 or 3.1.1, error message 1921 might be displayed for the UMSHTTPD service.	Stop the UMSHTTPD service.
(Japanese, Simplified and Traditional Chinese, and Korean only)  After upgrading from IBM Director 3.1 to IBM Director 4.20, in the Management Processor Assistant (MPA) task, distorted characters appear in the <b>Description</b> field of the Alert-Forwarding Profiles.	Make a note of the <b>Description</b> field contents before upgrading. After installing IBM Director 4.20, you must reenter the information in English. All of the input fields that are interpreted by the service processor must be provided in US ASCII.
If you performed the following upgrades, the UM Service tree (which is displayed in the "Simple Event Filter Builder" window) is obsolete and cannot be used to filter events:  1. From version 3.1 to version 3.1.1 2. From version 3.1.1 to version 4.1 3. From version 4.1 to version 4.11 4. From version 4.11 to version 4.12 5. From version 4.12 to version 4.20	Right-click the <b>UM Services</b> tree and click <b>Delete</b> . Use the Director Agent Services tree to filter events.
(Windows only) If you performed the following upgrades and then uninstalled IBM Director Agent, certain files are not uninstalled:  1. From version 3.1 or 3.1.1 to version 4.1 2. From version 4.1 to version 4.20	You can safely delete the following files: <ul style="list-style-type: none"> <li>• <i>d</i>:\Program Files\UMS\Director\bin\CimUrlCgi.log</li> <li>• <i>d</i>:\Program Files\UMS\Director\bin\UMSagent.In</li> <li>• <i>d</i>:\Program Files\UMS\Director\bin\verify.out</li> <li>• <i>d</i>:\Program Files\UMS\Director\websrv</li> <li>• <i>d</i>:\Program Files\UMS\endpoint\lcf_env.cm</li> <li>• <i>d</i>:\Program Files\UMS\endpoint\lcf_env.sh</li> <li>• <i>d</i>:\Program Files\UMS\httpserv\cgi-bin\CimCgi.log</li> </ul> where <i>d</i> is the drive letter of the hard disk on which you installed IBM Director Agent.

## Uninstallation

Table 29 describes problems that might occur when you uninstall IBM Director.

Table 29. Uninstallation problems

Symptom	Suggested action
(Windows only) Error message 1306 is displayed.	Modify the settings for the IBM Director Support Program Service (TWGIPC). If Web-based Access is installed, you also must modify the settings for the IBM Director Agent Web Server (DirWbs). For both services, set the startup type to <b>Manual</b> . Restart (reboot) the management server, and then begin the uninstallation again.
(Windows only) The following message is displayed: Apache.exe has generated errors and will be closed by Windows. You will need to restart the program.	Modify the settings for the IBM Director Support Program Service (TWGIPC) and the IBM Director Agent Web Server (DirWbs). For both services, set the startup type to <b>Manual</b> . Restart (reboot) the management server, and then begin the uninstallation again.
(Windows 2000 and Windows XP only) If you uninstall IBM Director Server, the following IBM Director Agent Web Server log files might be locked: <ul style="list-style-type: none"> <li>• apache_log</li> <li>• date.txt</li> <li>• stderr.log</li> </ul> where <i>date</i> is the date that the file was created.	If this occurs, a message is displayed stating that the file cannot be deleted. When you click <b>Retry</b> , the message is displayed again. This is a Windows timing issue with locked files, and it occurs very infrequently.
(Windows only) If you performed the following upgrades and then uninstalled IBM Director Agent, certain files are not uninstalled: <ol style="list-style-type: none"> <li>1. From version 3.1 or 3.1.1 to version 4.1</li> <li>2. From version 4.1 to version 4.20</li> </ol>	You can safely delete the following files: <ul style="list-style-type: none"> <li>• <i>d</i>:\Program Files\UMS\Director\bin\CimUrlCgi.log</li> <li>• <i>d</i>:\Program Files\UMS\Director\bin\UMSagent.In</li> <li>• <i>d</i>:\Program Files\UMS\Director\bin\verify.out</li> <li>• <i>d</i>:\Program Files\UMS\Director\webserv</li> <li>• <i>d</i>:\Program Files\UMS\endpoint\lcf_env.cm</li> <li>• <i>d</i>:\Program Files\UMS\endpoint\lcf_env.sh</li> <li>• <i>d</i>:\Program Files\UMS\httpserver\cgi-bin\CimCgi.log</li> </ul> where <i>d</i> is the drive letter of the hard disk on which you installed IBM Director Agent.

## IBM Director Server

Table 30 describes general problems that might occur on management servers.

Table 30. IBM Director Server problems

Symptom	Suggested action
<b>Alerts</b>	
If you use IBM Director 4.20 to manage a system running IBM Director Agent 3.1, you might receive frequent remote login alerts.	IBM Director Server communicates frequently with the service processors present in managed systems. If IBM Director Agent 3.1 is running on a server that contains a service processor, it generates an event every time the service processor is accessed.
<b>Databases</b>	
(Windows only) The Microsoft Jet database is full.	Migrate to a larger database such as IBM DB2, Oracle Server, or Microsoft SQL Server.

Table 30. IBM Director Server problems (continued)

Symptom	Suggested action
When an Oracle Server database is used, errors occur during the database configuration process.	Configure and start the Oracle TCP/IP listener before starting the database configuration task. If a failure occurs, check the configuration of the TCP/IP listener.
If you use Telnet from a system running Windows to access a management server running Linux, and then you run the <code>cfgdb</code> utility, messages overlay.	Before running the <code>cfgb</code> utility, set the environmental variable <code>term</code> to <code>vt100</code> . Then, maximize the Telnet window to its largest possible size.
(Linux only) If you are not logged in to IBM Director Console, typing the <code>cfgdb</code> command at a local command prompt causes an error.	Configure the database by performing one of the following procedures: <ul style="list-style-type: none"> <li>Use Telnet to access the management server, and then run the <code>cfgdb</code> command.</li> <li>From a command prompt on the management server, issue the <b>startx</b> command. Then, run the <b>cfgdb</b> command.</li> </ul>
(Linux only) When the IBM Director database is run locally on the management server and the management server is restarted, IBM Director Server fails to start. The <code>TWGServer.err</code> file reports a database initialization error.	<p>The <code>TWGserver</code> service might have started before the database service. Back up the <code>etc/init.d/TWGserver</code> script and save it to a safe location. Then, modify the <code>etc/init.d/TWGserver</code> script to make sure that the database service starts before the IBM Director service:</p> <p>For Red Hat Linux: Locate the following section in the script:</p> <pre># chkconfig: 35 90 10 # description: Starts and stops the IBM Director service.</pre> <p>90 is the start number and 10 is the stop number. Modify this section so that the <code>TWGserver</code> start number is greater than the start number for the database service, and the <code>TWGserver</code> stop number is greater than the stop number for the database service.</p> <p>For SUSE LINUX: Locate the following section in the script:</p> <pre>### BEGIN INIT INFO # Required-Start: \$network # Required-Stop: \$network # Default-Start: 3 5 # Default-Stop: 0 1 6 # Description: Starts and stops the IBM Director service. ### END INIT INFO</pre> <p>Add the database service to the <code>Required-Start</code> and <code>Required-Stop</code> lines. For example, for PostgreSQL, change the lines to read as follows:</p> <pre># Required-Start: \$network postgresql # Required-Stop: \$network postgresql</pre> <p>Save the modified script. Run the <b>chkconfig</b> command twice, once to remove the IBM Director service and then to add it back to the list of start and stop services.</p>
<b>Discovery</b>	
A BladeCenter discovery does not function correctly when multiple network interface cards (NICs) are enabled.	<p>Determine the NICs that are connected to the BladeCenter unit network. Disable all NICs except for one, which must be able to communicate with the BladeCenter management module. Perform the discovery. When the discovery is completed, reenabling the NICs that you disabled.</p> <p><b>Note:</b> You must do this each time you want to discover the BladeCenter unit and its components.</p>

Table 30. IBM Director Server problems (continued)

Symptom	Suggested action
<p>After you click <b>Discover All Systems</b>, an RXE-100 Remote Expansion Enclosure is not discovered.</p>	<p>To solve this problem, perform one of the following procedures:</p> <ul style="list-style-type: none"> <li>From IBM Director Console, click <b>Tasks</b> → <b>Discover Systems</b> → <b>Physical Platforms</b>; then, click <b>Discover All</b>.</li> <li>Right-click any blank space in the Group Contents pane and click <b>New</b> → <b>Physical Platforms</b>. The “Add Physical Platforms” window opens. Type the name and IP address of the Remote Supervisor Adapter that is attached to the RXE-100 Remote Expansion Enclosure; then, click <b>OK</b>.</li> </ul>
<p>(Managed systems running Linux only) When no default router is configured or a nonroutable private network is used, IBM Director might not discover systems.</p>	<p>Complete one of the following procedures:</p> <ul style="list-style-type: none"> <li>Seed the network in the System Discovery (IP) pane. Click <b>Options</b> → <b>Discovery Preferences</b>. Then, click <b>System Discovery (IP)</b>.</li> <li>Set a default router by issuing the following command: <code>route add default gw <i>IP_address</i></code></li> </ul> <p>where <i>IP_address</i> is your IP address. For more information, see the man page for the <b>route</b> command. Setting a default router enables the discovery of systems that are accessible using the specified router.</p>
<p>IBM Director Server does not discover SNMP devices.</p>	<p>Make sure that the following conditions are met:</p> <ul style="list-style-type: none"> <li>The management server is running the SNMP service. If it is not, another system on the same subnet must be running an SNMP agent. In that case, remove the management server as the seed device and add the system running the SNMP agent.</li> <li>The seed devices or other devices to be discovered are running SNMP agents.</li> <li>The community names that are specified in the “Discovery Preferences” window allow IBM Director to read both the following tables: <ul style="list-style-type: none"> <li>mib-2.system table of the devices to be discovered</li> <li>mib-2.ip.ipNetToMediaTable on the seed devices</li> </ul> </li> <li>Correct network masks have been configured for all managed systems that must be discovered.</li> <li>Correct addresses have been entered for the seed devices. The most effective seed devices are routers and domain name servers. To configure these devices, from IBM Director Console, click <b>Options</b> → <b>Discovery Preferences</b>. SNMP discovery does not discover all SNMP devices. If a device has not communicated with other managed systems, the device might not be discovered.</li> </ul>
<p><b>Encryption</b></p>	
<p>After you use the “Encryption Administration” window to change encryption settings, certain managed systems appear accessible but cannot be managed.</p>	<p>This might be due to one of the following circumstances:</p> <ul style="list-style-type: none"> <li>When you request a new key or a cipher algorithm, IBM Director must perform a presence check. This presence check might not be completed immediately. During the delay, IBM Director Server cannot manage the system.</li> <li>If you disable encryption on the management server, encrypted managed systems can no longer be managed. However, these systems might appear to be manageable for a certain period before they are displayed as locked.</li> </ul> <p>To ensure that the icons displayed in IBM Director Console accurately reflect the security state of the managed system, request a presence check.</p>

Table 30. IBM Director Server problems (continued)

Symptom	Suggested action
<b>Event actions</b>	
After a NIC on the management server is reconfigured, certain event actions fail.	IBM Director Server has lost contact with the managed systems that were discovered before the configuration change. From IBM Director Console, click <b>Tasks</b> → <b>Discover Systems</b> → <b>System Discovery</b> to rediscover the managed systems.
A timeout occurs during communications between IBM Director Server and IBM Director Console.	Working with large event action plans can cause network communication errors to occur. IBM Director Server takes a long time to process large requests from IBM Director Console. During this processing period, IBM Director Console waits for a response from IBM Director Server. When no response is received after 15 seconds, a timeout error is generated. This error might occur several times for intensive operations, such as importing or exporting large event action plans.  Despite the communication error, the event action plan works correctly.
<b>i5/OS</b>	
Shortly after IBM Director Server is started with encryption enabled using <b>Options</b> → <b>Encryption Administration</b> , IBM Director Server fails.	Make sure that JCE is enabled in the /QIBM/ProdData/Java400/jdk13/lib/security/java.security file. Then, restart IBM Director Server.
IBM Director Server fails to start when SSL is enabled in the TWGServer.prop file.	Make sure that the following conditions are met; then, restart IBM Director Server: <ul style="list-style-type: none"> <li>• A default server certificate is assigned in the Digital Certificate Manager *SYSTEM certificate store. The certificate is neither expired nor revoked.</li> <li>• You have installed a cumulative program temporary fix (PTF) package that includes 5722SS1 SI13495.</li> <li>• After installing the PTF, you enabled JCE in the /QIBM/ProdData/Java400/jdk13/lib/security/java.security file.</li> </ul>
IBM Director Server fails to start when the Japanese coded character set identifier (CCSID) 5026 is used.	Make sure that the job CCSID and locale match and that they are supported by Qshell. Consider using CCSID 5035 and locale JA_5035.  For more information, go to the iSeries Information Center at <a href="http://www.ibm.com/servers/eserver/iseries/infocenter">http://www.ibm.com/servers/eserver/iseries/infocenter</a> and search on National Language Support.
<b>Starting</b>	
(Linux only) Shortly after IBM Director Server is started, it enters an error state and the daemon.stderr file reports the following error:  Exception in thread "main"	Make sure that "localhost" is an alias for the loopback address 127.0.0.1 in the /etc/hosts file. Restart IBM Director Server.
(Windows Server 2003 only) When IBM Director Server starts for the first time on an ASF-capable system, the event log might contain traps or exceptions.	IBM Director Server completed installation before the system management bus (SMBus) was detected and the device driver installed.  When you install IBM Director Server or IBM Director Agent, be sure that the SMBus device driver is installed before you restart the system.

Table 30. IBM Director Server problems (continued)

Symptom	Suggested action
You are not sure whether IBM Director Server is running.	<p>To check whether the management server is running, complete one of the following procedures:</p> <ul style="list-style-type: none"> <li>• (i5/OS) From a Qshell command prompt, type the following command and press Enter: /QIBM/ProdData/Director/bin/twgstat</li> </ul> <p>The current status of IBM Director Server is displayed.</p> <ul style="list-style-type: none"> <li>• (Linux) From a command prompt, type the following command and press Enter: /opt/IBM/director/bin/twgstat -r</li> </ul> <p>The current status of IBM Director Server is displayed.</p> <ul style="list-style-type: none"> <li>• (Windows) Determine which of the following icons is displayed in the task bar in the lower-right corner of the screen. <ul style="list-style-type: none"> <li>– A green circle indicates that IBM Director Server is running.</li> <li>– A green triangle icon indicates that IBM Director Server is in the process of starting.</li> <li>– A red diamond icon indicates that IBM Director Server is not responding.</li> </ul> </li> </ul> <p>Do not attempt to start IBM Director Console until a green circle is displayed in the task bar.</p>

## IBM Director Console

Table 31 describes general problems that might occur on the management console.

Table 31. IBM Director Console problems

Symptom	Suggested action
<b>BladeCenter unit</b>	
After a blade server is installed in a BladeCenter chassis, a physical platform managed object (PPMO) associated with the blade server is not displayed in IBM Director Console.	Run the Inventory task on the BladeCenter chassis.
After a physical platform managed object is deleted, it reappears in IBM Director Console.	Delete the managed system or systems that are associated with the physical platform managed object.
<b>Databases</b>	
(Linux only) If you are not logged in to IBM Director Console, typing the <code>cfgdb</code> command at a local command prompt causes an error.	<p>Configure the database by performing one of the following procedures:</p> <ul style="list-style-type: none"> <li>• Use Telnet to access the management server, and then run the <code>cfgdb</code> command.</li> <li>• From a command prompt on the management server, issue the <code>startx</code> command. Then, run the <code>cfgdb</code> command.</li> </ul>
<b>Data displayed in windows</b>	
Some IBM Director Console windows display tables of data. The columns within these tables might not display the entire contents contained in them when the window opens.	To widen a column, drag the column border to resize it, or resize the entire window. The changes to the columns are not saved, and the next time the window is opened, you might have to resize the columns again.

Table 31. IBM Director Console problems (continued)

Symptom	Suggested action
<b>Dynamic groups criteria</b>	
When a dynamic group is created using certain criteria (such as the not-equal-to operator as part of the selected criteria), not all of the managed systems that meet those criteria are returned.	<p>Make sure that you use the correct criteria when you create the dynamic group. Each criterion searches only the rows in the inventory database with which it is associated.</p> <p>For example, when you select the following criterion: Inventory (PC)/SCSI Device/Device Type=TAPE</p> <p>IBM Director searches the inventory database for managed systems that have entries in the SCSI_DEVICE table. Then, IBM Director returns only the managed systems that have a value of TAPE in the DEVICE_TYPE column.</p> <p>When you select the following criterion: Inventory (PC)/SCSI Device/Device Type ^= TAPE</p> <p>IBM Director searches the inventory database for managed systems that have entries in the SCSI_DEVICE table. Then, IBM Director returns only the managed systems that do not have a value of TAPE in the DEVICE_TYPE column.</p> <p>Selecting the second criterion does not return all managed systems that do not have SCSI tape drives. It returns all managed systems that contain non-tape SCSI devices.</p>
<b>Event action plans</b>	
An event action plan is not displayed.	<p>When you apply an event action plan to a group, the event action plan is associated with <i>all</i> existing systems in the group. However, this group event action plan is not displayed as associated with each individual managed system that is part of the group. The event action plan is displayed as being applied to the group <i>only</i>.</p> <p>Complete the following steps to view the event action plans associated with the groups of managed systems:</p> <ol style="list-style-type: none"> <li>1. In IBM Director Console, click <b>Associations</b> → <b>Event Action Plans</b>.</li> <li>2. In the Groups pane, click <b>All Groups</b>.</li> <li>3. In the Group Category Contents pane, expand each group that has an event action plan applied to it and view the event action plans that are applied to the group.</li> </ol>
<b>Java Runtime Environment (JRE) Exceptions</b>	
Intermittent JRE exceptions occur.	Make sure that the management console has sufficient memory. Intermittent JRE exceptions might occur when you run IBM Director Console on systems that have insufficient memory. Sun Microsystems has acknowledged this problem. For more information about memory requirements, see “Hardware requirements” on page 13.
<b>Managed system</b>	
A question mark is displayed with the managed system icon.	Reestablish communication between IBM Director Server and IBM Director Agent on the managed system. Click <b>Tasks</b> → <b>Discover Systems</b> → <b>System Discovery</b> to rediscover the managed system.

Table 31. IBM Director Console problems (continued)

Symptom	Suggested action
<p>Managed systems are not displayed in IBM Director Console.</p>	<p>Make sure that the system is turned on, IBM Director Agent is running, and the network connection is reliable.</p> <p>Increase the network timeout value for both IBM Director Server and IBM Director Agent:</p> <ul style="list-style-type: none"> <li>• <b>Windows:</b> Run twgipccf.exe.</li> <li>• <b>Linux:</b> Using an ASCII text editor, open the ServiceNodeLocal.properties file (located in the /opt/IBM/director/data directory), and modify the value of ipc.timeouts. By default, it is set to 15 seconds.</li> </ul> <p>Stop and restart IBM Director Agent to ensure that the new network timeout takes effect.</p>
<p>A request for access fails and the managed system remains locked.</p>	<p>Make sure that the following conditions are met:</p> <ul style="list-style-type: none"> <li>• You are using the correct user ID and password.</li> <li>• If the managed system accepts encrypted communications only, make sure that the management server has encryption enabled also.</li> <li>• If the managed system is running Linux, the password encryption is set to either Message Digest 5 (MD5) or Data Encryption Standard (DES).</li> </ul>
<p>When you request access to a managed system running Linux, access is not granted.</p>	<p>If the operating-system password encryption method is set to MD5 (Message Digest 5) when you install IBM Director Agent, salt values that contain only two characters might be generated. IBM Director requires that the salt values be eight characters in length. Use the <b>passwd</b> command to reset the password for the account that is used to access the managed system.</p>
<p>After using imaging to deploy a system, duplicate managed systems are displayed in IBM Director Console.</p> <p>When using imaging, make sure that the instance of IBM Director Agent that is being cloned has never been started.</p>	<p>Perform one of the following procedures on the duplicate managed system:</p> <p><b>Linux:</b> Complete the following steps:</p> <ol style="list-style-type: none"> <li>1. Using an ASCII text editor, open the ServiceNodeLocal.properties file (located in the /opt/IBM/director/data directory), and delete the line that begins with the following string: ipc.UID=</li> <li>2. Delete the TWGagent.uid file, which is located in the /etc/TWAgent directory.</li> </ol> <p><b>Windows:</b> Complete the following steps:</p> <ol style="list-style-type: none"> <li>1. Remove the following registry key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName\TWGMachineID</li> <li>2. Delete the twgmach.id file. If you installed IBM Director Agent in the default location, this file is in the \\Program Files\IBM\data directory.</li> </ol>

Table 31. IBM Director Console problems (continued)

Symptom	Suggested action
<p>(Linux only) When no default router is configured or a nonroutable private network is used, IBM Director might not add discovered systems on these networks to the IBM Director Console Group Contents pane.</p>	<p>Complete one of the following procedures to ensure that the managed systems are displayed in IBM Director Console:</p> <ul style="list-style-type: none"> <li>Seed the network in the System Discovery (IP) pane. Click <b>Options</b> → <b>Discovery Preferences</b>. Then, click <b>System Discovery (IP)</b>.</li> <li>Set a default router by issuing the following command:  <pre>route add default gw IP_address</pre> </li> </ul> <p>where <i>IP_address</i> is your IP address. For more information, see the man page for the <b>route</b> command. Setting a default router enables the discovery of systems that are accessible using the specified router.</p>
<p>After you use the “Encryption Administration” window to change encryption settings, certain managed systems appear accessible but cannot be managed.</p>	<p>This might be due to one of the following circumstances:</p> <ul style="list-style-type: none"> <li>When a new key or a new cipher algorithm is requested, a presence check is forced by IBM Director. This presence check might not be completed immediately. During this delay, IBM Director Server cannot manage the system.</li> <li>When encryption is disabled on the management server, encrypted managed systems can no longer be managed. However, these systems might appear to be manageable for a certain period before they are displayed as locked.</li> </ul> <p>To ensure that the icons displayed in IBM Director Console accurately reflect the security state of the managed system, request a presence check.</p>
<b>Starting</b>	
<p>When you try to start IBM Director Console, the following error message is displayed:</p> <p>An IO error occurred while connecting to the IBM Director Server.</p>	<p>Before you start IBM Director Console, make sure that IBM Director Server is running.</p> <ul style="list-style-type: none"> <li>(i5/OS) From a Qshell command prompt, type the following command and press Enter:  <pre>/QIBM/ProdData/Director/bin/twgstat</pre> </li> </ul> <p>The current status of IBM Director Server is displayed.</p> <ul style="list-style-type: none"> <li>(Linux) From a command prompt, type the following command and press Enter:  <pre>/opt/IBM/director/bin/twgstat -r</pre> </li> </ul> <p>The current status of IBM Director Server is displayed.</p> <ul style="list-style-type: none"> <li>(Windows) Determine which of the following icons is displayed in the task bar in the lower-right corner of the screen. <ul style="list-style-type: none"> <li>– A green circle indicates that IBM Director Server is running.</li> <li>– A green triangle icon indicates that IBM Director Server is in the process of starting.</li> <li>– A red diamond icon indicates that IBM Director Server is not responding.</li> </ul> </li> </ul> <p>Do not attempt to start IBM Director Console until a green circle is displayed in the task bar.</p>

Table 31. IBM Director Console problems (continued)

Symptom	Suggested action
Errors occur during attempts to log on to the management server using IBM Director Console.	<p>Make sure that the following conditions are met:</p> <ul style="list-style-type: none"> <li>• Both the management server and IBM Director Server are running.</li> <li>• The management server name, user ID, and password are valid. (For systems running Windows, you must qualify the user ID with either the domain or the local computer name of the management server.)</li> <li>• You have a connection from the management console to TCP port 2033 on the management server.</li> <li>• IBM Director Console and IBM Director Server are the same version.</li> <li>• (If SSL is used) Both the management console and the management server are using compatible data link connection classes and parameters in the TWGConsole.prop and TWGServer.prop files.</li> <li>• (If SSL is used) The certification chain of the certificate authority that issued the server certificate is trusted in the keystore that is used by the management console.</li> </ul>
<b>Time zone</b>	
The wrong time zone is displayed.	When the time zone setting is changed on the managed system, the time that is shown in the event viewer is not adjusted. Restart the managed system to ensure that the correct time zone is displayed.

## IBM Director Agent

Table 32 describes symptoms of problems that might occur on managed systems.

Table 32. IBM Director Agent problems

Symptom	Suggested action
(Linux only) Shortly after IBM Director Agent starts, it enters an error state and the daemon.stderr file reports the following error: Exception in thread "main"	Make sure that "localhost" is an alias for the loopback address 127.0.0.1 in the /etc/hosts file. Restart IBM Director Agent.
(Windows Server 2003 only) When IBM Agent starts for the first time on an ASF-capable system, the event log might contain traps or exceptions.	<p>IBM Director Agent completed installation before the system management bus (SMBus) was detected and the device driver installed.</p> <p>When you install IBM Director Server or IBM Director Agent, be sure that the SMBus device driver is installed before you restart the system.</p>
When you request access to a managed system running Linux, access is not granted.	If the operating-system password encryption method is set to MD5 (message digest 5) when you install IBM Director Agent, salt values that contain only two characters might be generated. IBM Director requires that the salt values be eight characters in length. Use the <b>passwd</b> command to reset the password for the account that is used to access the managed system.

Table 32. IBM Director Agent problems (continued)

Symptom	Suggested action
(Red Hat Linux only) On rare occasions, when the Inventory task attempts to collect data on Red Hat Package Manager (RPM) packages, IBM Director Agent times out and fails.	<p>Stop and restart IBM Director Agent.</p> <p>If you do not need the RPM package data, clear the check box in the Inventory pane of the “Server Preferences” window; then, run the Inventory task again.</p> <p>If you do need the RPM package data, you must create a symbolic link. From the command prompt on the managed system, using an account with root privileges, type the following commands:</p> <pre>ln -s /usr/lib/librpm-x.so /usr/lib/librpm-4.0.3.so ln -s /usr/lib/librpmio-x.so /usr/lib/librpmio-4.0.3.so ln -s /usr/lib/librpmdb-x.so /usr/lib/librpmdb-4.0.3.so</pre> <p>where x is the version of the files on the managed system.</p>

## Managed systems running Windows

Table 33 describes symptoms of Windows-specific problems that might occur on managed systems running Windows.

Table 33. Managed systems running Windows problems

Symptom	Suggested action
<p>The Remote Access Connection Manager service fails to start and the following error message is displayed:</p> <p>The service cannot be started, either because it is disabled or because it has no enabled devices associated with it.</p>	<p>This problem is solved by a Microsoft update. See Microsoft Knowledge Base article 830459 for more information.</p>
(Windows 2000 only) After cluster failover, cluster failback, or disk drive unplug operations, a managed system returns invalid resource-monitor information for Windows Performance Monitors or Logical Disks.	<p>Install Microsoft Windows 2000 Service Pack 4.</p>
<p>A managed system returns invalid data values for the following:</p> <ul style="list-style-type: none"> <li>• Windows Performance Monitors</li> <li>• LogicalDisk or Windows Performance Monitors</li> <li>• PhysicalDisk</li> </ul>	<p>This problem is solved by a Microsoft update. See Microsoft Knowledge Base article 827439 for more information.</p>
(Windows 2000 only) The event log is full. This problem occurs on servers when NetBIOS is enabled and IBM Director is installed. Errors are generated until the event log is full.	<p>Uninstall and then reinstall the device driver for the NIC.</p>

Table 33. Managed systems running Windows problems (continued)

Symptom	Suggested action
(Windows 2000 Server only) After IBM Director Server is installed, the following error is displayed in the event log when the server is restarted:  The open procedure for service PerfDisk in the DLL C:\WINNT\System32\perfdisk.dll has taken longer than the established wait time to be completed.	Use the <b>regedit</b> command to modify the following key entry and change the decimal value to 30000:  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PerfDisk\Performance key "Open Timeout"  This gives the system enough time to complete the startup task before starting the PERF counters.
(Windows 2000 with Internet Information Services (IIS) installed) An event ID 2003 warning message appears in the application event log when you start System Monitor and add counters.	Microsoft has identified this as a problem. For more information, see Microsoft Knowledge Base Article 267831.
The following report is generated:  Win32_DiskDrive.Size is less than Win32_DiskPartition.Size for a removable medium that has been formatted as a single partition.	The following hard disk drives are not supported by Windows: <ul style="list-style-type: none"> <li>• Optical</li> <li>• Iomega</li> <li>• Jaz</li> </ul> Microsoft identified this as a Windows Management Instrumentation (WMI) problem.
A PCI adapter with logical disks cannot be stopped using the "Unplug or Eject Hardware" window.	Install Microsoft Windows 2000 Service Pack 4.

## IBM Director tasks

Table 34 describes symptoms of problems that might occur when you are using IBM Director tasks other than Software Distribution.

Table 34. IBM Director task problems

Symptom	Suggested action
<b>Active PCI Manager</b>	
The Active PCI Manager task appears to be available after you upgrade to IBM Director 4.20, but its subtasks are not working.	Complete the following steps to solve this problem: <ol style="list-style-type: none"> <li>1. From Add/Remove Programs, remove all previous versions of Active PCI Manager.</li> <li>2. Reinstall IBM Director 4.20. Be sure to install the Active PCI Manager component from the Server Plus Pack.</li> </ol>
<b>BladeCenter Assistant</b>	
(IBM @server BladeCenter HS40 only) In the BladeCenter Assistant task, if you click <b>VRM</b> to view the voltage regulator module (VRM) information, two rows of information are displayed.	Ignore the second VRM row that contains a value of 0.0; that VRM does not exist. This error does not generate an event or cause any functional problems.
<b>Common Information Model (CIM) Browser</b>	
When you attempt to enumerate a system running Windows, large amounts of CIM data are returned, causing errors in the CIM Browser.	Do not attempt to enumerate the instances of the following classes: <ul style="list-style-type: none"> <li>• root/cimv2:CIM_DirectoryContainsFile</li> <li>• root/cim2:Win32_Subdirectory</li> </ul> Those CIM classes have instances for every file and directory on every disk in your server. If you attempt to enumerate these classes, the managed system or management server might run out of memory.

Table 34. IBM Director task problems (continued)

Symptom	Suggested action
<b>Inventory</b>	
Field-replaceable unit (FRU) information does not appear when inventory is collected.	<p>If a system is not connected to the Internet when IBM Director Agent is installed, the FRU inventory might be empty. To populate the FRU inventory, run the GETFRU command. For more information, see Appendix B, "Obtaining FRU data files using the GETFRU command," in the <i>IBM Director 4.20 Systems Management Guide</i>.</p> <p>In addition, make sure that the GETFRU command can reach the IBM Support FTP site through your firewall. For the GETFRU command to run successfully, the managed system must have firewall access through a standard FTP port.</p>
The Inventory task times out when it is run against a server that contains a Remote Supervisor Adapter II.	Make sure that the Remote Supervisor Adapter II device driver is installed on the managed system.
The ServeRAID inventory tables are missing information.	<p>When IBM Director Server collects inventory from a managed system running IBM Director Agent 3.1 and either Windows NT 4.0 or Windows 2000, the following inventory is not collected:</p> <ul style="list-style-type: none"> <li>• ServeRAID Controllers</li> <li>• ServeRAID Disk Drives</li> <li>• ServeRAID Enclosures</li> <li>• ServeRAID Logical Drives</li> </ul> <p>Consider upgrading to IBM Director Agent 4.20.</p>
(Red Hat Linux only) On rare occasions, when the Inventory task attempts to collect data on Red Hat Package Manager (RPM) packages, IBM Director Agent times out and fails.	<p>Stop and restart IBM Director Agent.</p> <p>If you do not need the RPM package data, clear the check box in the Inventory pane of the "Server Preferences" window; then, run the Inventory task again.</p> <p>If you do need the RPM package data, you must create a symbolic link. From the command prompt on the managed system, using an account with root privileges, type the following commands:</p> <pre>ln -s /usr/lib/librpm-x.so /usr/lib/librpm-4.0.3.so ln -s /usr/lib/librpmio-x.so /usr/lib/librpmio-4.0.3.so ln -s /usr/lib/librpmdb-x.so /usr/lib/librpmdb-4.0.3.so</pre> <p>where x is the version of the files on the managed system.</p>
<b>Management Processor Assistant</b>	
When you use the Communications configuration subtask, connection information is not displayed.	<p>Complete one of the following procedures:</p> <ul style="list-style-type: none"> <li>• Exit Management Processor Assistant and wait a few minutes. Start the Management Processor Assistant task and try again.</li> <li>• Click <b>Communications configuration</b>. In the left pane, click <b>Global settings</b> to refresh the Communications configuration subtask for each selected system.</li> </ul>
<p>(Japanese, Korean, Simplified Chinese, and Traditional Chinese only)</p> <p>In the Management Processor Assistant (MPA) task, distorted characters appear in the <b>Description</b> field of the Alert-Forwarding Profiles. This problem occurs after you have upgraded from IBM Director 3.1 to IBM Director 4.20.</p>	Make a note of the <b>Description</b> field contents before upgrading. After installing IBM Director 4.20, you must reenter the information in English. All of the input fields that are interpreted by the service processor must be provided in US ASCII.

Table 34. IBM Director task problems (continued)

Symptom	Suggested action
<b>Mass Configuration</b>	
When you use the Mass Configuration task to configure Asset ID™, the configuration fails.	The managed system does not have sufficient data space. When the size of the configuration is larger than that of the remaining data space, the configuration fails (although there is no indication that a failure has occurred). This is a limitation of the data save area. Make sure that, for each byte of data, the managed system has the same amount of space in the data save area.
<b>Network Configuration</b>	
When you use the Network Configuration task to change the computer name of a managed system, the computer name is not displayed correctly.	Be sure to restart the managed system.
(Managed system running Windows Server 2003) When you run the Network Configuration task and view the WINS pane, the IP addresses for the primary and secondary Windows Internet Naming Service (WINS) servers are reversed.	This is caused by a Microsoft implementation of a CIM class. The correct IP addresses are assigned in the system Network Properties.
<b>Remote Control</b>	
When you use a non-English-language keyboard during a remote-control session, some of the keys might not work.	Make sure that the inventory has been collected before you use the Remote Control task.
The Remote Control task fails when both the following conditions are true: <ul style="list-style-type: none"> <li>You are running the task against a managed system that is behind a firewall.</li> <li>You are simultaneously distributing a software package to that managed system.</li> </ul>	The Remote Control and Software Distribution tasks both use session support to increase data transmission. Session support within TCP/IP causes data to flow through a nonreserved port that is different from the one that IBM Director typically uses for communication. Most firewalls do not allow the data to be transmitted through this other port. You can disable session support by creating an INI file on the managed system. In the IBM\Director\bin directory on the managed system, create a file named tcpip.ini that contains the following command: <pre>SESSION_SUPPORT=0</pre> <p>If more than one TCP/IP option is selected in the network driver configuration of the managed system, you must create an INI file for each entry. Name these files tcpip.ini, tcpip2.ini, tcpip3.ini, and so on. After creating the files, restart the managed system.</p>
<b>Resource Monitors</b>	
(Windows only) When you run the Resource Monitors tasks against multiple managed systems, incorrect attribute names might be displayed for the network adapters.	The incorrect attribute names are displayed in the Available Resources pane of the "Resource Monitors" window, when you click <b>Director Agent → TCP/IP Monitors</b> . <p>To view the correct attribute names for the network adapters, click <b>Director Agent → Windows Performance Monitors → Network Interface</b>.</p>
<b>SNMP Browser</b>	
When a Management Information Base (MIB) file attribute value is set to a hexadecimal, octal, or binary value, the file fails.	Make sure that all of the values have been converted and are being added in a decimal format.

Table 34. IBM Director task problems (continued)

Symptom	Suggested action
You cannot change an attribute value for a MIB file.	<p>Make sure that the following conditions are met:</p> <ul style="list-style-type: none"> <li>• IBM Director uses a community name that allows write access to the MIB file.</li> <li>• The MIB file is writable.</li> <li>• The MIB file has a value that you can set to be displayed in the SNMP Browser.</li> <li>• The compiled MIB file is associated with the value that you want to change.</li> </ul>
Trap destinations are missing from the SNMP agent table.	A table displays only the first trap destination in the SNMP configuration interface when multiple communities and traps are associated with each community. The IBM Director inventory stores only the first value of an array-valued property, such as the SNMP trap destination.

## Software Distribution

Table 35 describes problems that might occur when you use Software Distribution.

Table 35. Software Distribution problems

Symptom	Suggested action
The software package creation fails.	Check the available disk space on the management console. Packages are created on the management console. If the management-console disk space is insufficient, the package creation fails.
<p>The Software Distribution task fails when both the following conditions are true:</p> <ul style="list-style-type: none"> <li>• You are distributing a software package to a managed system that is behind a firewall.</li> <li>• You are simultaneously running a Remote Control task on that managed system.</li> </ul>	<p>The Remote Control and Software Distribution tasks both use session support to increase data transmission. Session support within TCP/IP causes data to flow through a nonreserved port that is different from the one that IBM Director typically uses for communication. Most firewalls do not allow the data to be transmitted through this other port. You can disable session support by creating an INI file on the managed system. In the IBM\Director\bin directory on the managed system, create a file named tcpip.ini that contains the following command:</p> <pre>SESSION_SUPPORT=0</pre> <p>If more than one TCP/IP option is selected in the network driver configuration of the managed system, you must create an INI file for each entry. Name these files tcpip.ini, tcpip2.ini, tcpip3.ini, and so on. After creating the files, restart the managed system.</p>
<p>When a software package is distributed using a redirector share, the following error message is displayed:</p> <pre>I/O error, file (\\server\share) \ (package name)not found on managed system (system name)</pre>	This problem occurs if you manually delete a software package from the redirector share. To deleted packages from the share, you must use the “File Distribution Servers Manager” window. Right-click the <b>Software Distribution</b> task and click <b>File Distribution Servers Manager</b> .
<p>When you attempt to export a software-distribution package to a network share, the following error message is displayed:</p> <pre>Unable to export package.</pre>	The Software Distribution task does not support exporting packages to a network share. Modify the operation to export the package to a local drive.

Table 35. Software Distribution problems (continued)

Symptom	Suggested action
(Windows only) Software packages are streamed from the management server, although a file-distribution server is configured for use by the managed systems.	<p>Make sure that one of the following conditions is met:</p> <ul style="list-style-type: none"> <li>The file-distribution server is a member of the same domain as the management server.</li> <li>The file-distribution server has a trust relationship with the domain where the management server is located.</li> </ul>
(Linux only) If you export a software-distribution package to Software Package Bundle (SPB) format and then reimport the package, an error message is displayed.	<p>Change the permission levels. From the local command prompt, type the following command:</p> <pre>chmod 644 filename.spb</pre>
<p>(Japanese only, on managed systems running Windows) In the “Distribution Preferences” window, the <b>Share Name</b> field is filled in by default with the following example share name:</p> <pre>¥system¥share</pre> <p>However, when you press the yen key, the <b>Share Name</b> field incorrectly displays the backslash (\) symbol.</p>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>Do not overwrite or delete the example share name.</li> <li>Retain the yen symbols in the example and replace only system and share with the system name and share name that you want to use.           <p><b>Note:</b> If you press the yen key, do not use the backslashes; the backslashes cause redirected distribution to fail.</p> </li> <li>Close the “Distribution Preferences” window; then, reenter this window, and retain the yen symbols in the <b>Share Name</b> field example.</li> </ol>
<p>(Korean only, on managed systems running Windows) In the “Distribution Preferences” window, the <b>Share Name</b> field is filled in with the following example share name by default:</p> <pre>₩system₩share</pre> <p>where ₩ represents the won symbol.</p> <p>However, when you press the won key, the <b>Share Name</b> field incorrectly displays the backslash (\) symbol.</p>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>Do not overwrite or delete the example share name.</li> <li>Retain the won symbols in the example and replace only system and share with the system name and share name that you want to use.           <p><b>Note:</b> If you press the won key, do not use the backslashes; the backslashes cause redirected distribution to fail.</p> </li> <li>Close the “Distribution Preferences” window; then, reenter this window, and retain the won symbols in the <b>Share Name</b> field example.</li> </ol>
(File-distribution server running i5/OS only) Redirected software distribution using an FTP share fails.	<p>To use an FTP-based share for redirected software distribution, the FTP configuration on the file-distribution server might need to be modified. Use the Change FTP Attributes command (CHGFTP) to set the initial name format to *PATH and specify the initial directory. Stop and restart the FTP server. This changes the default FTP settings for all managed systems that use the file-distribution server.</p>
After you upgrade to Software Distribution (Premium Edition), you cannot export a package that was created with Director Update Assistant.	<p>Delete the software package that was created with Software Distribution (Standard Edition). Re-import the package using Director Update Assistant in Software Distribution (Premium Edition).</p>

## Web-based Access

Table 36 describes symptoms of problems that might occur when you use Web-based Access.

Table 36. Web-based Access problems

Symptom	Suggested action
(Windows XP or Windows Server 2003 only) A message is displayed stating that Java Virtual Machine (JVM) is needed.	Install a Java Virtual Machine (JVM) from Sun Microsystems.
After repeated installations, there are problems logging in to the managed system using Netscape Navigator.	When you uninstall IBM Director Agent, be sure to save the configuration data. This saves the old Secure Sockets Layer (SSL) certificate and allows the login to the IBM Director Agent Web Server to successfully complete after IBM Director Agent is reinstalled.
After you log in to Microsoft Internet Explorer, a Java security warning is displayed.	If you are using Microsoft Internet Explorer with the Sun Java Plug-in, additional prompts appear when you log in to a managed system. After you log in to Microsoft Internet Explorer, a Java Security Warning is displayed. Select <b>Grant this session</b> . The Java Plug-in requires authentication information. Type the same information that you used for the Microsoft Internet Explorer login.
When you install Web-based Access on a managed system that is running Apache Web Server, Web-based Access is unavailable. An error message is displayed indicating that the page cannot be found.	Web-based Access and Apache Web Server use the same default connector ports. You must modify the Web-based Access configuration files. If you installed IBM Director Agent in the default location, these files are located in the Program Files\IBM\Director\websrv\conf directory. Complete the following steps to resolve this problem: <ol style="list-style-type: none"> <li>1. Stop the IBM Director Agent Web Server service.</li> <li>2. Modify the server.xml file: <ul style="list-style-type: none"> <li>• Change the server port to a port that is not already in use by another application. By default, the server port is set to 8005.</li> <li>• Change the connector port to a port that is not already in use by another application. By default, it is set to 8009.</li> </ul> </li> <li>3. Modify the workers.properties file. Change the connector port to a port that is not already in use by another application. By default, it is set to 8009.</li> <li>4. Modify the tomcat.conf file. Change the connector port to a port that is not already in use by another application. By default, it is set to 8009.</li> <li>5. Restart the IBM Director Agent Web Server service.</li> </ol>
(Traditional and Simplified Chinese only) When you open Web-based Access in a Netscape Web browser, the Chinese characters might be displayed as boxes.	Complete the following steps to ensure that Chinese characters are displayed properly: <ol style="list-style-type: none"> <li>1. Install the Java Plug-in 1.4.1 that is available from Sun Microsystems.</li> <li>2. Check the Windows Display Properties settings to make sure that they are set correctly for Chinese language display.</li> </ol>
When you use event bindings, events are not delivered correctly.	If you use the Health service (a Configuration task on the Tasks page) to add event bindings, the system from which you access Web-based Access must have its regional settings set to English. If the regional settings are not set to English, the event filter strings are in the non-English language, and events are not delivered correctly.

## Systems running double-byte character set languages

Table 37 describes symptoms of problems that might occur when you are running IBM Director on systems using the following double-byte character set (DBCS) languages: Japanese, Korean, Simplified Chinese, and Traditional Chinese.

Table 37. Systems running double-byte character set languages problems

Symptom	Suggested action
<p>(Japanese, Simplified and Traditional Chinese, and Korean only)</p> <p>After upgrading from IBM Director 3.1 to IBM Director 4.20, in the Management Processor Assistant (MPA) task, distorted characters appear in the <b>Description</b> field of the Alert-Forwarding Profiles.</p>	<p>Make a note of the <b>Description</b> field contents before upgrading. After installing IBM Director 4.20, you must reenter the information in English. All of the input fields that are interpreted by the service processor must be provided in US ASCII.</p>
<p>(i5/OS) IBM Director Server fails to start when the Japanese coded character set identifier (CCSID) 5026 is used.</p>	<p>Make sure that the job CCSID and locale match and that they are supported by Qshell. Consider using CCSID 5035 and locale JA_5035.</p> <p>For more information, go to the iSeries Information Center at <a href="http://www.ibm.com/servers/eserver/series/infocenter">http://www.ibm.com/servers/eserver/series/infocenter</a> and search on National Language Support.</p>
<p>(Japanese only, on managed systems running Windows) In the “Distribution Preferences” window, the <b>Share Name</b> field is filled in by default with the following example share name: ¥¥system¥share</p> <p>However, when you press the yen key, the <b>Share Name</b> field incorrectly displays the backslash (\) symbol.</p>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>1. Do not overwrite or delete the example share name.</li> <li>2. Retain the yen symbols in the example and replace only system and share with the system name and share name that you want to use. <b>Note:</b> If you press the yen key, do not use the backslashes; the backslashes cause redirected distribution to fail.</li> <li>3. Close the “Distribution Preferences” window; then, reenter this window, and retain the yen symbols in the <b>Share Name</b> field example.</li> </ol>
<p>(Korean only, on managed systems running Windows) In the “Distribution Preferences” window, the <b>Share Name</b> field is filled in with the following example share name by default: ₩₩system₩share</p> <p>where ₩ represents the won symbol.</p> <p>However, when you press the won key, the <b>Share Name</b> field incorrectly displays the backslash (\) symbol.</p>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>1. Do not overwrite or delete the example share name.</li> <li>2. Retain the won symbols in the example and replace only system and share with the system name and share name that you want to use. <b>Note:</b> If you press the won key, do not use the backslashes; the backslashes cause redirected distribution to fail.</li> <li>3. Close the “Distribution Preferences” window; then, reenter this window, and retain the won symbols in the <b>Share Name</b> field example.</li> </ol>
<p>(Traditional and Simplified Chinese only)</p> <p>When you open Web-based Access in a Netscape Web browser, the Chinese characters might be displayed as boxes.</p>	<p>Complete the following steps to ensure that Chinese characters are displayed properly:</p> <ol style="list-style-type: none"> <li>1. Install the Java Plug-in 1.4.1 that is available from Sun Microsystems.</li> <li>2. Check the Windows Display Properties settings to make sure that they are set correctly for Chinese language display.</li> </ol>



---

## Chapter 15. Getting help and technical assistance

If you need help, service, or technical assistance or just want more information about IBM products, you will find a wide variety of sources available from IBM to assist you. This appendix contains information about where to go for additional information about IBM and IBM products, what to do if you experience a problem with your xSeries or IntelliStation system, and whom to call for service, if it is necessary.

---

### Before you call

Before you call, make sure that you have taken these steps to try to solve the problem yourself:

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system is turned on.
- Use the troubleshooting information in your system documentation, and use the diagnostic tools that come with your system. Information about diagnostic tools is in the *Hardware Maintenance Manual and Troubleshooting Guide* on the IBM *xSeries Documentation* CD or in the *IntelliStation Hardware Maintenance Manual* at the IBM Support Web site.
- Go to the IBM Support Web site at <http://www.ibm.com/pc/support/> to check for technical information, hints, tips, and new device drivers or to submit a request for information.

You can solve many problems without outside assistance by following the troubleshooting procedures that IBM provides in the online help or in the publications that are provided with your system and software. The information that comes with your system also describes the diagnostic tests that you can perform. Most xSeries and IntelliStation systems, operating systems, and programs come with information that contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the information for the operating system or program.

---

### Using the documentation

Information about your IBM xSeries or IntelliStation system and preinstalled software, if any, is available in the documentation that comes with your system. That documentation includes printed books, online books, readme files, and help files. See the troubleshooting information in your system documentation for instructions for using the diagnostic programs. The troubleshooting information or the diagnostic programs might tell you that you need additional or updated device drivers or other software. IBM maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. To access these pages, go to <http://www.ibm.com/pc/support/> and follow the instructions. Also, you can order publications through the IBM Publications Ordering System at <http://www.elink.ibm.com/public/applications/publications/cgibin/pbi.cgi>.

---

## Getting help and information from the World Wide Web

On the World Wide Web, the IBM Web site has up-to-date information about IBM xSeries and IntelliStation products, services, and support. The address for IBM xSeries information is <http://www.ibm.com/eserver/xseries/>. The address for IBM IntelliStation information is <http://www.ibm.com/pc/intellistation/>.

You can find service information for your IBM products, including supported options, at <http://www.ibm.com/pc/support/>.

---

## Software service and support

Through IBM Support Line, you can get telephone assistance, for a fee, with usage, configuration, and software problems with xSeries servers, IntelliStation workstations, and appliances. For information about which products are supported by Support Line in your country or region, go to <http://www.ibm.com/services/sl/products/>.

For more information about Support Line and other IBM services, go to <http://www.ibm.com/services/>, or go to <http://www.ibm.com/planetwide/> for support telephone numbers. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

---

## Part 6. Appendixes



---

## Appendix A. IBM Director Agent — IBM Director Server security

This chapter contains information about IBM Director Agent — IBM Director Server security. It includes an overview of authentication, procedures for securing managed systems, and information about key management.

---

### How authentication works

Integrated into IBM Director is a security mechanism by which a managed system can authenticate any management server attempting to access it. Authentication enables IBM Director Agent to accept commands only from an IBM Director Server that is trusted (that is, authorized to manage it). Authentication protects managed systems from access by unauthorized management servers or rogue managed-system applications.

The IBM Director authentication process is based on two interlocking concepts:

- Digital-signature certification
- Security state of the managed system

### Digital-signature certification

IBM Director authentication is based on the Digital Signature Algorithm (DSA). DSA is the public-key algorithm specified by the Digital Signature Standard of the National Institute of Standards and Technology. It enables the holder of a public key to verify the signature for a digital document that has been signed by a holder of the corresponding private key. In an IBM Director environment, it works in the following way:

1. IBM Director Server attempts to access IBM Director Agent. IBM Director Server bids the public keys that correspond to the private keys it holds.
2. IBM Director Agent checks these keys. If it considers the keys to be trusted, IBM Director Agent replies with a challenge that consists of one of the trusted public keys and a random data block.
3. IBM Director Server generates a digital signature of the random data block using the private key that corresponds to the public key included in the challenge. IBM Director Server sends the signature back to IBM Director Agent.
4. IBM Director Agent uses the public key to verify that the signature is a valid signature for the random data block. If the signature is valid, IBM Director Agent grants access to IBM Director Server.

This digital signature scheme has the following benefits:

- The public keys stored on the managed systems can be used only for verifying access.
- Using a random data block for signing makes replay attacks unusable.
- Generating a private key corresponding to a given public key is cryptographically improbable, requiring  $2^{128}$  or more operations to accomplish.

### Security state of the managed system

A managed system is in either an unsecured or secured state. A managed system is *unsecured* when any management server can access it and perform functions on it. A managed system is *secured* when only an authorized (trusted) management server can access it.

The initial security state of IBM Director Agent depends on the underlying operating system.

Table 38. Initial security state of IBM Director Agent

Operating system	Security state
AIX	Secured by default during installation of IBM Director Agent.
i5/OS	Secured by default during installation of IBM Director Agent.
Linux	Secured by default during installation of IBM Director Agent.
NetWare	Unsecured by default. Must be secured manually or during discovery. See "Securing managed systems" on page 235 for more information.
Windows	Can be secured during installation of IBM Director Agent.

If IBM Director Agent is not secured during installation of IBM Director Agent, you can secure the managed system manually or during discovery.

**Note:** The IBM Director Agent running on a management server is secured automatically. It has a trust relationship only with the IBM Director Server installed on the same server.

On managed systems running Windows, the security state is determined by the `secin.ini` file. If the `secin.ini` file is initialized as unsecured, any management server can access the managed system and establish a trust relationship with IBM Director Agent. IBM Director Server establishes a trust relationship by giving IBM Director Agent a copy of its public key.

When the managed system has been secured by a management server, only that management server, any management servers that had previously established a trust relationship, and any future management servers that successfully request access are able to access the managed system.

## Where security information is stored

The information needed for authentication is stored in files on both the management server and the managed systems.

The public keys are stored in `dsaxxxx.pub` files, where `xxxxx` is a unique identifier. The private keys held by IBM Director Server are stored in `dsaxxxx.pvt` files. For example, the `dsa23ef4.pub` file contains the public key corresponding to the private key stored in the `dsa23ef4.pvt` file.

On systems running Windows, the secured/unsecured state data is stored in the `secin.ini` file, which is generated when you first start IBM Director Server or IBM Director Agent. On management servers, this file is initialized as secured; on managed systems, it is initialized as either secured or unsecured, depending on which options were selected during the installation of IBM Director Agent.

By default, the files are located in the following directories.

Operating system	Directory
Linux operating systems for AMD64 and 32-bit systems	/opt/IBM/director/data
Linux operating systems for Intel Itanium and IBM iSeries and pSeries	/opt/ibm/director/data
i5/OS	/QIBM/UserData/Director/data
NetWare	d:\IBM\Director
Windows	d:\Program Files\IBM\Director\Data

where *d* is the drive letter of the hard disk on which IBM Director is installed and IBM Director is installed in the default location.

## How the keys and secin.ini files work together

When you first start IBM Director Server, it randomly generates a matching set of public and private key files (dsa\*.pub and dsa\*.pvt files). The secin.ini file is generated and initialized as secure.

The initial security state of a managed system depends on the following factors:

- Which operating system it is running
- Which features were selected during the installation of IBM Director Agent

Managed systems running NetWare are set to the unsecured state automatically. For all other managed systems, the initial security state depends on which features are selected when IBM Director Agent is installed. If either encryption or agent/server security is selected, the managed system is set automatically to the secured state.

While a managed system is in the unsecured state, it accepts a public key from *every* management server that attempts to access it. Through this process, the managed system establishes trust relationships with those management servers.

If a management server secures that unsecured managed system, it gives that managed system a copy of its public key *and* its secin.ini file, which is initialized as secure. After this has occurred, the managed system no longer accepts any new public keys from management servers. However, the managed system continues to grant access to any management server whose public key is stored on the managed system.

---

## Securing managed systems

There are several ways IBM Director Server can secure managed systems: during discovery, during the installation of IBM Director, and by manually copying the key files to managed systems.

### Automatically securing unsecured systems

To configure IBM Director Server to secure unsecured managed systems automatically, in IBM Director Console click **Options** → **Discovery Preferences**; then, select the **Automatically secure unsecured systems** check box.

## Manually securing a managed system

**Note:** Use this procedure in the following situations:

- You suspect that a rogue management server was introduced into an IBM Director environment before all managed systems were secured, and you want to resolve any possible security risks.
- You want to establish trust relationships between a managed system and multiple management servers.

Complete the following steps to manually secure a managed system running Windows or NetWare. You can use this procedure to secure either an unsecured or secured system:

1. If you have not done so already, install and start IBM Director Server. IBM Director Server creates a `dsa*.pub` and `dsa*.pvt` file, as well as a `secin.ini` file set to secure.
2. Copy the `dsa*.pub` and `secin.ini` files to a file server or other accessible location.

**Note:** If you want to authorize more than one IBM Director Server to manage a system, copy the `dsa*.pub` files from each. Only one copy of `secin.ini` is necessary.

3. If IBM Director Agent installed on the managed system has not been started yet, continue to step 5. Otherwise, stop IBM Director Agent. From a command prompt, type the following command and press Enter:

<b>For NetWare</b>	<code>unload twgipc</code>
<b>For Windows</b>	<code>net stop twgipc</code>

4. Delete all existing `dsa*.pub` files from the managed system.
5. Place the `dsa*.pub` and `secin.ini` files (that you copied in step 2) into one of the following directories:

<b>For NetWare</b>	<code>d:\IBM\Director</code>
<b>For Windows</b>	<code>d:\Program Files\IBM\director\data</code>

where *d* is the hard disk where IBM Director Agent is installed, and IBM Director Agent is installed in the default directory.

6. To restart IBM Director Agent, type one of the following commands and press Enter:

<b>For NetWare</b>	<code>load twgipc</code>
<b>For Windows</b>	<code>net start twgipc</code>

After IBM Director Agent starts, the managed system is secure; it permits *only* authorized IBM Director Servers (that is, the ones whose `dsa*.pub` file you copied to the managed system) to manage it.

You can automate this procedure by using logon scripts or other automated execution mechanisms.

---

## Changing access or security states

This section provides information about gaining access to a secure managed system, removing access to a managed system, and adding another management server to an existing secure environment.

### Accessing a secure managed system

If a managed system is secure but the management server to which you are connected does not have authorization to access it, the managed system is displayed in the Group Contents pane of IBM Director Console with a padlock icon beside it.

Complete the following steps to access a secure managed system from an unauthorized management server:

1. In IBM Director Console, right-click the managed system to which you do not have access.
2. Click **Request Access**. The “Request Access to Systems” window opens.

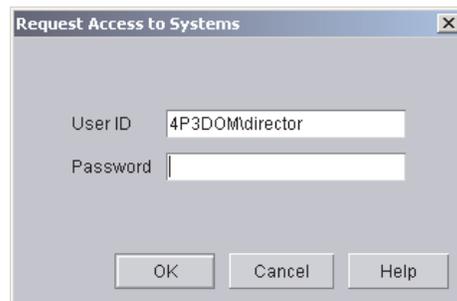


Figure 120. “Request Access to Systems” window

3. To access the system, type an authorized user ID and password; then, click **OK**.

**Notes:**

- a. The user ID must have administrator privileges on the managed system.
- b. The dsa\*.pub files in the director\data directory on the managed system are the public key files used for authentication. They are largely unreadable binary files. However, the first string of characters in the file is the name of the management server that is trusted by the managed system.

You also can copy the dsa\*.pub file from the management server to the managed system. After the managed system is restarted, it trusts the new management server.

### Removing access to a managed system

To revoke the ability of a management server to access a managed system, delete the dsa\*.pub file from the director\data directory on the managed system. Complete the following steps:

1. Change to the Director\Data directory on the managed system.
2. Using an ASCII text editor, view each dsa\*.pub file. The first characters in a dsa\*.pub file are of the form DSAxxxx, where xxxx is the name of the management server.
3. Locate the dsa\*.pub file for the management server that you want to unauthorize, and delete it.

4. To stop IBM Director Agent, from a command prompt, type one of the following commands and press Enter:

<b>For i5/OS</b>	/qibm/userdata/director/bin/twgend
<b>For Linux</b>	/opt/IBM/director/twgstop
<b>For NetWare</b>	unload twgipc
<b>For Windows</b>	net stop twgipc

5. To restart IBM Director Agent, type one of the following commands and press Enter:

<b>For i5/OS</b>	/qibm/userdata/director/bin/twgend
<b>For Linux</b>	/opt/IBM/director/twgstart
<b>For NetWare</b>	load twgipc
<b>For Windows</b>	net start twgipc

After IBM Director Agent starts, the management server whose dsa\*.pub file you removed is no longer able to access the managed system.

## Adding a trusted management server to an existing secure environment

To add another trusted management server to an existing secure environment, you can perform one of the following procedures:

- Set up the new server, install IBM Director Server, and copy the new server dsa\*.pvt file to a trusted management server. Stop and restart IBM Director Server on the trusted management server. As IBM Director Server initializes, it delivers the dsa\*.pub file corresponding to the new dsa\*.pvt file to all of its trusting managed systems. This causes the managed systems to trust the new management server.
- Set up the new server, install IBM Director Server, and copy the dsa\*.pvt file from an existing trusted management server. This enables the new management server to authenticate itself immediately to the managed systems that trusted the existing management server. The new management server also is trusted by the older management server.

---

## Key management

This section provides information about determining the origin of a key and recovering lost keys.

### Determining the origin of a public or private key

The public and private key files are binary files, but they contain textual data that indicates their origin. If a dsa\*.pub or dsa\*.pvt file is printed using the type command at a command prompt, the following data is displayed in the first line:

```
DSAKeytypeString
```

where:

- *Keytype* indicates the type of the key. “P” denotes private, and “p” denotes public.
- *String* is the name of the management server that generated the key file.

For example, DSAPzydeco indicates a private key file generated by a management server named zydeco, and DSApzydeco indicates the public key file generated by the same management server.

## Recovering lost public and private key files

It is *very important* to back up and protect the dsa\*.pvt files. If they are lost, you cannot regenerate these files.

If a private key file is lost, you must repeat one of the previously described procedures for initializing security or adding a new trusted management server, either using another existing trusted dsa\*.pvt key or the new key generated by the management server when it restarts without its private key file. See “Adding a trusted management server to an existing secure environment” on page 238.

If a public key file is lost, you can regenerate it by having the management server that holds the corresponding private key discover, add, or access any unsecured managed system. The public key file is generated on the managed system. The management server does not require the dsa\*.pub file that corresponds to its dsa\*.pvt file; the private key file includes all the information from the public key files.



---

## Appendix B. Terminology summary and abbreviation list

This appendix provides a summary of IBM Director terminology and a list of abbreviations that are used in IBM Director documentation.

---

### IBM Director terminology summary

The following terminology is used in the IBM Director documentation.

A *system* is a server, workstation, desktop computer, or mobile computer. An *SNMP device* is a device (such as a network printer) that has SNMP installed or embedded. An *IBM Director environment* is a group of systems managed by IBM Director.

IBM Director software is made up of three main components:

- IBM Director Server
- IBM Director Agent
- IBM Director Console

The hardware in an IBM Director environment is referred to in the following ways:

- A *management server* is a server on which IBM Director Server is installed.
- A *managed system* is a system on which IBM Director Agent is installed.
- A *management console* is a system on which IBM Director Console is installed.

*Extensions* are tools for advanced server management that extend the functionality of IBM Director. Such tools include the IBM Server Plus Pack, Software Distribution (Premium Edition), Remote Deployment Manager, and others.

(Management servers running Windows only) The *IBM Director service account* is an operating-system user account on the management server. This is the account under which the IBM Director Service runs.

The *database server* is the server on which the database application is installed.

The system from which you invoke DIRCMD, the IBM Director command-line interface, is a *DIRCMD client*.

---

### Abbreviations

The following table lists abbreviations that are used in the IBM Director documentation.

Table 39. Abbreviations used in IBM Director

Abbreviation	Definition
<b>A</b>	
ACPI	Advanced Configuration and Power Interface
ASCII	American Standard Code for Information Interchange
ASF	Alert Standard Format
ASM	Advanced System Management
ASM PCI Adapter	Advanced System Management PCI adapter

Table 39. Abbreviations used in IBM Director (continued)

<b>Abbreviation</b>	<b>Definition</b>
ASM processor	Advanced System Management processor
<b>B</b>	
BIOS	basic input/output system
<b>C</b>	
CCSID	coded character set identifier
CIM	Common Information Model
CIMOM	CIM Object Manager
CPW	commercial processing workload
CRC	cyclic redundancy check
CSM	IBM Cluster Systems Management
CSV	comma-separated value
<b>D</b>	
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DIMM	dual inline memory module
DMI	Desktop Management Interface
DMTF	Distributed Management Task Force
DNS	Domain Name System
DSA	Digital Signature Algorithm
<b>E</b>	
EEPROM	electrically erasable programmable read-only memory
<b>F</b>	
FRU	field-replaceable unit
FTMI	fault tolerant management interface
FTP	File Transfer Protocol
<b>G</b>	
GB	gigabyte
Gb	gigabit
GMT	Greenwich mean time
GUI	graphical user interface
GUID	globally unique identifier
<b>H</b>	
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
<b>I</b>	
IETF	Internet Engineering Task Force
IFS	integrated file system
IIS	Microsoft Internet Information Services
I/O	input/output

Table 39. Abbreviations used in IBM Director (continued)

<b>Abbreviation</b>	<b>Definition</b>
IP	Internet Protocol
IPC	interprocess communication
IPMI	Intelligent Platform Management Interface
IPX	Internetwork Packet Exchange
ISDN	integrated services digital network
ISMP	integrated system management processor
<b>J</b>	
JCE	IBM Java Cryptography Extension
JDBC	Java Database Connectivity
JDK	Java Development Kit
JFC	Java Foundation Classes
JRE	Java Runtime Environment
JVM	Java Virtual Machine
<b>K</b>	
KB	kilobyte
KBps	kilobytes per second
Kb	kilobits
Kbps	kilobits per second
KVM	keyboard/video/mouse
<b>L</b>	
LAN	local area network
LED	light-emitting diode
<b>M</b>	
MAC	media access control
MB	megabyte
MBps	megabytes per second
Mb	megabit
Mbps	megabits per second
MD5	message digest 5
MDAC	Microsoft Data Access Control
MHz	megahertz
MIB	Management Information Base
MIF	Management Information Format
MMC	Microsoft Management Console
MPA	Management Processor Assistant
MPCLI	Management Processor Command-Line Interface
MSCS	Microsoft Cluster Server
MSDE	Microsoft Data Engine
MST	Microsoft software transformation
MTU	maximum transmission unit

Table 39. Abbreviations used in IBM Director (continued)

Abbreviation	Definition
<b>N</b>	
NAS	network attached storage
NetBIOS	Network Basic Input/Output System
NIC	network interface card
NNTP	Network News Transfer Protocol
NTFS	Windows NT 4.0 file system
NVRAM	nonvolatile random access memory
<b>O</b>	
ODBC	Open Database Connectivity
OID	object ID
<b>P</b>	
PCI	peripheral component interconnect
PCI-X	peripheral component interconnect-extended
PDF	Portable Document Format
PET	Platform Event Trap
PFA	Predictive Failure Analysis
PIN	personal identification number
POST	power-on self-test
PPMO	physical platform managed object
PPP	Point-to-Point Protocol
PTF	program temporary fix
<b>R</b>	
RAID	redundant array of independent disks
RAM	random access memory
RDM	IBM Remote Deployment Manager
RPM	(1) Red Hat Package Manager (2) revolutions per minute
<b>S</b>	
SCSI	small computer system interface
SHA	Secure Hash Algorithm
SID	(1) security identifier (2) Oracle system identifier
SLP	Service Location Protocol
SMART	Self-Monitoring, Analysis, and Reporting Technology
SMBIOS	System Management BIOS
SMBus	system management bus
SMI	System Management Information
SMS	Microsoft Systems Management Server
SMTP	Simple Mail Transfer Protocol
SNA	Systems Network Architecture

Table 39. Abbreviations used in IBM Director (continued)

<b>Abbreviation</b>	<b>Definition</b>
SNMP	Simple Network Management Protocol
SPB	software package bundle
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
SSM	IBM Scalable Systems Manager
<b>T</b>	
TAP	Telocator Alphanumeric Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TTL	time to live
<b>U</b>	
UDP	User Datagram Protocol
UID	unique ID
UIM	upward integration module
UNC	universal naming convention
USB	Universal Serial Bus
UUID	universal unique identifier
<b>V</b>	
VMM	IBM Virtual Machine Manager
VPD	vital product data
VRM	voltage regulator module
<b>W</b>	
WAN	wide area network
WfM	Wired for Management
WINS	Windows Internet Naming Service
WMI	Windows Management Instrumentation
<b>X</b>	
XML	Extensible Markup Language



---

## Appendix C. 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.*

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.

---

## Edition notice

© Copyright International Business Machines Corporation 2004. All rights reserved.

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

---

## Trademarks

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

Active PCI	OS/400
AIX	PowerPC
Asset ID	Predictive Failure Analysis
BladeCenter	pSeries
DB2	Redbooks
DB2 Universal Database	ServeRAID
e-business logo	ServerProven
@server	SurePOS
IBM	ThinkCentre
IBM i5/OS	ThinkPad
IBM Virtualization Engine	Tivoli
IntelliStation	Tivoli Enterprise
iSeries	Tivoli Enterprise Console
Netfinity	TotalStorage
NetView	Wake on LAN
NetVista	xSeries

Intel and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

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

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

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

Red Hat, the Red Hat “Shadow Man” logo, and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc., in the United States and other countries.

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

---

# Glossary

## A

**Active PCI Manager task.** An IBM Director extension available in the Server Plus Pack that can be used to manage all PCI and PCI-X adapters in a managed system. The Active PCI Manager task provides two subtasks in IBM Director: Fault Tolerant Management Interface (FTMI) and Slot Manager (previously released under the name Active PCI Manager).

**Advanced System Management (ASM) interconnect.** A feature of IBM service processors. It enables you to connect up to 24 servers to one service processor, thus eliminating the need for multiple modems, telephones, and LAN ports. It provides strong out-of-band management functions, including system power control, service processor event log management, firmware updates, alert notification, and user profile configuration.

**Advanced System Management (ASM) interconnect network.** A network of IBM servers created by using the ASM interconnect feature. The servers are connected through RS-485 ports. When servers containing ISMPs and ASM processors are connected to such a network, IBM Director can manage them out-of-band.

**Advanced System Management (ASM) PCI adapter.** An IBM service processor that is built into the system board of Netfinity 7000 M10 and 8500R servers. It also was available as an option that could be installed in a server that contained an ASM processor. When an ASM PCI adapter is used with an ASM processor, the ASM PCI adapter acts as an Ethernet gateway, while the ASM processor retains control of the server. When used as a gateway service processor, the ASM PCI adapter can communicate with other ASM PCI adapters and ASM processors only.

**Advanced System Management (ASM) processor.** A service processor built into the system board of mid-range Netfinity and early xSeries servers. IBM Director can connect out-of-band to an ASM processor located on an ASM interconnect; an ASM PCI adapter, a Remote Supervisor Adapter, or a Remote Supervisor II must serve as the gateway service processor.

**alert.** A notification of an event occurrence. If an event action plan is configured to filter a specific event, when that event occurs, an alert is generated in response to that event.

**alert-forwarding profile.** In the IBM Director Management Processor Assistant and BladeCenter Assistant tasks, a profile that specifies where remote alerts for the service processor are sent. Alert forwarding can ensure that alerts are sent, even if a

managed system experiences a catastrophic failure, such as an operating-system failure.

**alert standard format (ASF).** A specification created by the Distributed Management Task Force (DMTF) that defines remote-control and alerting interfaces that can best serve a client system in an environment that does not have an operating system.

**anonymous command execution.** Execution of commands on a target system as either system account (for managed systems running Windows) or root (for managed systems running Linux). You can restrict anonymous command execution by disabling this feature and always requiring a user ID and password.

**ASF.** See alert standard format.

**ASM interconnect gateway.** See gateway service processor.

**Asset ID task.** An IBM Director task that can be used to track lease, warranty, user, and system information, including serial numbers. You also can use the Asset ID feature to create personalized data fields to track custom information.

**association.** (1) A way of displaying the members of a group in a logical ordering. For example, the Object Type association displays the managed objects in a group in folders based on their type. (2) A way to display additional information about the members of the group. For example, the Event Action Plans association displays any event action plans applied to the managed objects in the group in an Event Action Plan folder.

## B

**basic input/output system (BIOS).** The personal computer code that controls basic hardware operations, such as interactions with diskette drives, hard disk drives, and the keyboard. The Configuration/Setup Utility program is a menu-driven utility that is part of the BIOS code that comes with a server. You can start it with F1 during a specific point in the server startup (by watching the screen for a message about it).

**BIOS.** See basic input/output system.

**blade server.** An IBM @server BladeCenter server. Each BladeCenter chassis can hold up to 14 of these high-throughput, two-way, SMP-capable Xeon-based servers.

**BladeCenter Assistant task.** An IBM Director task that can be used to configure and manage BladeCenter units.

**BladeCenter chassis.** A BladeCenter unit that acts as an enclosure. This 7-U modular chassis can contain up to 14 blade servers. It enables the individual blade servers to share resources such as the management, switch, power, and blower modules.

**BladeCenter Deployment wizard.** A BladeCenter Assistant subtask that can be used to configure BladeCenter chassis, including setting up security protocols, enabling network protocols, and assigning IP addresses to the management and switch modules. It also can create a chassis detect-and-deploy profile that will automatically configure new BladeCenter chassis when they are added to the IBM Director environment.

**BladeCenter Diagnostics.** A Real Time Diagnostics subtask that can be used to diagnose problems in the components that are present in a BladeCenter unit.

**bottleneck.** In the Capacity Manager task, a condition in which one or more performance analysis monitors meet or exceed their preset threshold settings.

## C

**Capacity Manager task.** An IBM Director extension, available in the Server Plus Pack, that can be used to plan resource management and monitor managed-system hardware performance. It can identify bottlenecks and potential bottlenecks, recommend ways to improve performance through performance analysis reports, and forecast performance trends.

**chassis detect-and-deploy profile.** A profile that IBM Director automatically applies to all new BladeCenter chassis when they are discovered. The profile settings include management module name, network protocols, and static IP addresses. If Remote Deployment Manager is installed on the management server, the chassis detect-and-deploy profile also can include deployment policies.

**CIM.** See Common Information Model.

**CIM Browser task.** An IBM Director task that can provide in-depth information that you can use for problem determination or developing a systems-management application using the CIM layer.

**Common Information Model (CIM).** A standard defined by the Distributed Management Task Force (DMTF). CIM is a set of methodologies and syntaxes that describes the management features and capabilities of computer devices and software.

**component association.** In the IBM Director Rack Manager task, a function that can make a managed system or device rack-mountable when the inventory collection feature of IBM Director does not recognize the managed system or device. The function associates the system or device with a predefined component.

## D

**data encryption standard (DES).** A block cipher algorithm that can be used to encrypt data transmitted between managed systems and the management server. Designed by the National Bureau of Standards, DES enciphers and deciphers data using a 64-bit key.

**database server.** The server on which the database application and database used with IBM Director Server is installed.

**deployment policy.** A policy that associates a specific bay in a BladeCenter chassis with an RDM noninteractive task. When a blade server is added to or replaced in the bay, IBM Director automatically runs the RDM task.

**DES.** See data encryption standard.

**Desktop Management Interface (DMI).** A specification from the Desktop Management Task Force (DMTF) that establishes a standard framework for managing networked computers. DMI includes hardware and software, desktop systems, and servers, and it defines a model for filtering events. DMI provides a common path to access information about all aspects of a managed system. It is mappable to existing management protocols such as Simple Network Management Protocol (SNMP).

**Diffie-Hellman key exchange.** A security protocol developed by Whitfield Diffie and Martin Hellman in 1976. This protocol enables two users to exchange a secret digital key over an insecure medium. IBM Director uses the Diffie-Hellman key exchange protocol when establishing encrypted sessions between the management server and managed system.

**digital signature algorithm (DSA).** A security protocol used by IBM Director. DSA uses a pair of keys (one public and one private) and a one-way encryption algorithm to provide a robust way of authenticating users and systems. If a public key can successfully decrypt a digital signature, a user can be sure that the signature was encrypted using the private key.

**DirAdmin.** A Windows operating-system group that is created automatically when IBM Director Server is installed. By default, members of the DirAdmin group have basic administrative privileges in the IBM Director environment.

**DIRCMD.** The command-line interface to IBM Director. It enables members of the super-user group to use a command-line prompt to access, control, and gather information from IBM Director Server.

**DIRCMD client.** The system from which a system administrator invokes DIRCMD.

**DirSuper.** A Windows operating-system group that is created automatically when IBM Director Server is installed. The IBM Director service account is assigned automatically to the DirSuper group. Members of the DirSuper group have the same privileges as the DirAdmin group, as well as the ability to permit or restrict users' access to IBM Director.

**discovery.** The process by which IBM Director Server identifies and establishes connections with systems on which IBM Director Agent is installed. In a discovery operation, the management server sends out a discovery request and waits for responses from managed systems. The managed systems wait for this request and respond to the management server.

**discovery, BladeCenter chassis.** The process by which IBM Director Server identifies and establishes communication with a BladeCenter chassis. If the management server and the BladeCenter chassis are on the same subnet, IBM Director uses Service Location Protocol (SLP) to discover the BladeCenter chassis automatically. Otherwise, a network administrator must use IBM Director Console to create a BladeCenter chassis managed object manually.

**discovery, broadcast.** A type of discovery supported by IBM Director, in which the management server sends out either a general broadcast packet over the LAN or a broadcast packet to a specific subnet.

**discovery, broadcast relay.** A type of discovery supported by IBM Director, in which the management server sends a special discovery request to a particular managed system, instructing the managed system to perform a discovery operation on the local subnet using a general broadcast. This method of discovery enables the management server to discover TCP/IP and IPX systems when the systems are not directly reachable by broadcast packets because of network configuration.

**discovery, multicast.** A type of discovery supported by IBM Director, in which the management server sends a packet to a specified multicast address. Multicasts are defined with a maximum time to live (TTL) and are discarded when the TTL expires. Multicast discovery is available only for TCP/IP systems.

**discovery, SNMP.** A type of discovery supported by IBM Director, in which IBM Director sends discovery requests to seed addresses (such as routers and name servers). The address tables found on the specified devices are then searched; the search continues until no additional SNMP devices are found.

**discovery, unicast.** A type of discovery supported by IBM Director, in which the management server sends a directed request to a specific address or range of addresses. This method of discovery is useful in networks where both broadcasts and multicasts are filtered.

**DMI.** See Desktop Management Interface.

**DMI Browser task.** An IBM Director task that can provide in-depth information about DMI components. Used primarily for systems management, DMI does not support management of network devices, such as bridges, routers, and printers, as SNMP does.

**dynamic group.** See group, dynamic.

## E

**event.** An occurrence of a predefined condition relating to a specific managed object. There are two kinds of events: alert and resolution. An alert is the occurrence of a problem relating to a managed object. A resolution is the occurrence of a correction or a solution to a problem.

**event action.** The action that IBM Director takes in response to a specific event or events. In the Event Action Plan Builder, you can customize an event action type by specifying certain parameters and saving the event action. You must assign the customized event action (and an event filter) to an event action plan before IBM Director can execute the event action.

**event action plan.** A user-defined plan that determines how IBM Director will manage certain events. An event action plan comprises one or more event filters and one or more customized event actions. The event filters specify which events are managed, and the event actions specify what happens when the events occur.

**Event Action Plan wizard.** An IBM Director Console wizard that can be used to create a simple event action plan.

**event-data substitution variable.** A variable that can be used to customize event-specific text messages for certain event actions.

**event filter.** A filter that specifies the event criteria for an event action plan. Events must meet the criteria specified in the event filter in order to be processed by the event action plan that the filter is assigned to.

**extension.** See IBM Director extension.

## F

**Fault Tolerant Management Interface (FTMI).** An Active PCI Manager subtask that can be used to manage PCI and PCI-X network adapters on managed systems. FTMI can be used to view network adapters that are members of fault-tolerant groups. It also can be used to perform offline, online, failover, and eject operations on the displayed adapters.

**field-replaceable unit (FRU).** A component of an IBM system that can be replaced in the field by a service

technician. Each FRU is identified by a unique seven-digit alphanumeric code.

**file-distribution server.** In the Software Distribution task, an intermediate server that is used to distribute a software package when the redirected-distribution method is used.

**File Transfer task.** An IBM Director task that can be used to transfer files from one location (managed system or management server) to another. It also can be used to synchronizes file, directories, or drives.

**forecast.** In the Capacity Manager task, a function that can provide a prediction of future performance of a managed system using past data collected on that managed system.

**FRU.** See field-replaceable unit.

**FTMI.** See Fault Tolerant Management Interface.

## G

**gateway service processor.** A service processor that relays alerts from service processors on an ASM interconnect network to IBM Director Server.

**group.** A logical set of managed objects. Groups can be dynamic, static, or task-based.

**group, dynamic.** A group of managed systems or managed objects based on a specific criterion, for example, a group of managed systems running Windows 2000 with Service Pack 3 or later. IBM Director automatically adds or removes managed systems or managed objects to or from a dynamic group when their attributes or properties change.

**group, static.** A user-defined group of managed systems or managed objects, for example, all servers in a particular department. IBM Director does not automatically update the contents of a static group.

**group, task-based.** A dynamic group based on the types of tasks for which the group of managed objects is enabled. For example, selecting Rack Manager in the Available Tasks pane includes only those managed objects that can be used with the Rack Manager task.

**GUID.** See Universal Unique Identifier.

## H

**Hardware Status task.** An IBM Director task that can be used to view managed-system and managed-device hardware status from the management console. The Hardware Status task notifies you whenever a managed system or device has a hardware status change by displaying an icon in the lower-right corner of the IBM Director Console interface. Whenever a managed system or device generates a hardware event, the

Hardware Status task also adds the system or device to the applicable hardware status group (critical, warning, or information).

## I

**IBM Director Agent.** A component of IBM Director software. When IBM Director Agent is installed on a system, the system can be managed by IBM Director. IBM Director Agent transfers data to the management server using several network protocols, including TCP/IP, NetBIOS, IPX, and SNA.

**IBM Director Console.** A component of IBM Director software. When installed on a system, it provides a graphical user interface (GUI) that you can use to access IBM Director Server. IBM Director Console transfers data to and from the management server using TCP/IP.

**IBM Director database.** The database that contains the data stored by IBM Director Server.

**IBM Director environment.** The complex, heterogeneous environment managed by IBM Director. It encompasses systems, BladeCenter chassis, software, SNMP devices, and more.

**IBM Director extension.** A tool that extends the functionality of IBM Director. IBM Director extensions include the IBM Director Server Plus Pack, Remote Deployment Manager, Software Distribution, and others.

**IBM Director Server.** The main component of IBM Director software. When installed on the management server, it provides basic functions such as discovery of the managed systems, persistent storage of configuration and management data, an inventory database, event listening, security and authentication, management console support, and administrative tasks.

**IBM Director Server Plus Pack.** A portfolio of IBM Director extensions specifically designed for use with xSeries and Netfinity servers. It includes Active PCI Manager, Capacity Manager, Rack Manager, Software Rejuvenation, and System Availability.

**IBM Director Server service.** A service that runs automatically on the management server and provides the server engine and application logic for IBM Director.

**IBM Director service account.** The Windows operating-system account that is associated with the IBM Director Server service.

**in-band communication.** Communication that occurs through the same channels as data transmissions, for example, the interprocess communication that occurs between IBM Director Server, IBM Director Agent, and IBM Director Console.

**integrated system management processor (ISMP).**

A service processor built into the system board of some xSeries servers. The successor to the ASM processor, the ISMP does not support in-band communication in systems running NetWare. For IBM Director Server to connect out-of-band to an ISMP, the server containing the ISMP must be installed on an ASM interconnect network. The gateway service processor must be a Remote Supervisor Adapter or a Remote Supervisor Adapter II.

**interprocess communication (IPC).** A method by which threads and processes can transfer data and messages among themselves. Interprocess communication is used to transfer data and messages between IBM Director Server and IBM Director Agent, as well as IBM Director Agent and service processors. It also is called in-band communication

**inventory-software dictionary.** In the Inventory task, a file that tracks the software installed on managed systems in a network. The software-dictionary file contains predefined software profiles that recognize most standard software packages after they are installed. If you have software installed on managed systems that does not correspond to a predefined software profile included with IBM Director, you can edit the software-dictionary file to update your software inventory.

**Inventory task.** An IBM Director task that can be used to collect data about the hardware and software installed on a managed system.

**IPC.** See interprocess communication.

**IPMI.** See Intelligent Platform Management Interface.

**IPMI baseboard management controller.** Definition

**ISMP.** See integrated system management processor.

## J

**job.** In Scheduler, a single noninteractive task or set of noninteractive tasks scheduled to run at a later time.

## K

**keyboard/video/mouse (KVM).** A select button on a BladeCenter server bay.

**KVM.** See keyboard/video/mouse.

## L

**light path diagnostics.** An IBM technology present in xSeries servers. It constantly monitors selected features. If a failure occurs, a light-emitting diode (LED) is lit to indicate that a specific component or subsystem needs to be replaced.

## M

**MAC address.** See media access control (MAC) address.

**managed group.** A group of systems or objects managed by IBM Director.

**managed object.** An item managed by IBM Director. In IBM Director Console, a managed object is represented by an icon that shows its type (such as chassis, cluster, system, or scalable system, for example).

**managed object ID.** A unique identifier for each managed object. It is the key value used by IBM Director database tables.

**managed system.** A system (server, desktop computer, workstation, or mobile computer) on which IBM Director Agent is installed. Such a system is managed by IBM Director.

**managed system, secured.** A managed system that can be accessed only by an authorized management server.

**managed system, unsecured.** A managed system that can be accessed by any management server.

**management console.** A system (server, desktop computer, workstation, or mobile computer) on which IBM Director Console is installed.

**management module.** The BladeCenter component that handles systems-management functions. It configures the chassis and switch modules, communicates with the blade servers and all I/O modules, multiplexes the keyboard/video/mouse (KVM), and monitors critical information about the chassis and blade servers.

**Management Processor Assistant (MPA).** An IBM Director task that can be used to configure, monitor, and manage service processors installed in Netfinity and xSeries servers.

**Management Processor Assistant (MPA) Agent.** An IBM Director Agent feature that enables in-band communication with the service processors installed in Netfinity and xSeries servers. It also handles in-band alert notification for service processors installed in managed systems running NetWare.

**management server.** The server on which IBM Director Server is installed.

**media access control (MAC) address.** A standardized data-link layer address for every port or device that is connected to a LAN. Other devices in the network use MAC addresses to locate specific ports and to create and update routing tables and data structures.

**Message Browser.** An IBM Director Console window that displays alerts that are sent to IBM Director Console.

**Microsoft Cluster Browser task.** An IBM Director task that can be used to perform the following operations:

- Display the structure, nodes, and resources associated with a Microsoft Cluster Server (MSCS) cluster
- Determine the status of a cluster resource
- View the associated properties of the cluster resources

**Microsoft Management Console (MMC).** An application that provides a graphical user interface and a programming environment in which consoles (collections of administrative tools) can be created, saved, and opened. It is part of the Microsoft Platform Software Development Kit and is available for general use. On managed systems running Windows, the MMC is installed at the same time as Web-based Access.

**MMC.** See Microsoft Management Console.

**MPA.** See Management Processor Assistant.

**multicast discovery.** See discovery, multicast.

## N

**nonvolatile random-access memory (NVRAM).** Random access memory (storage) that retains its contents after the electrical power to the computer is shut off.

**notification.** See alert.

**NVRAM.** See nonvolatile random-access memory.

## O

**out-of-band communication.** Communication that occurs through a modem or other asynchronous connection, for example, service processor alerts sent through a modem or over a LAN. In an IBM Director environment, such communication is independent of the operating system and interprocess communication (IPC).

## P

**partition.** See scalable partition.

**PCI.** See peripheral component interconnect.

**PCI-X.** See peripheral component interconnect-extended.

**peripheral component interconnect (PCI).** A computer bussing architecture that defines electrical and physical standards for electronic interconnection.

**peripheral component interconnect-extended (PCI-X).** An enhanced computer bussing architecture that defines electrical and physical standards for electronic interconnection. PCI-X enhances the PCI standard by doubling the throughput capability and providing new adapter-performance options while maintaining backward compatibility with PCI adapters.

**PFA.** See Predictive Failure Analysis.

**physical platform.** An IBM Director managed object that represents a single physical chassis or server that has been discovered through the use of the Service Location Protocol.

**plug-in.** See IBM Director extension.

**POST.** See power-on self-test.

**power-on self-test.** A diagnostic testing sequence that is run by the BIOS when a system is turned on. The POST determines whether the RAM, disk drives, peripheral devices, and other hardware components are properly working.

**Predictive Failure Analysis (PFA).** An IBM technology that periodically measures selected attributes of component activity. If a predefined threshold is met or exceeded, a warning message is generated.

**private key.** A central component of the digital-signature algorithm. Each management server holds a private key and uses it to generate digital signatures that managed systems use to authenticate access by management servers.

**Process Management task.** An IBM Director task that manages individual processes on managed systems. Specifically, you can start, stop, and monitor processes and set up process monitors to generate an event whenever an application changes state. You also can issue commands on managed systems.

**process monitor.** A Process Management subtask that can be used to check for when a specified application process starts, stops, or fails to start running during a specified period of time after system startup or after the monitor is sent to a managed system.

**process task.** A Process Management subtask that can be used to simplify the running of programs and processes. You can predefine a command that can be run on a managed system or group by dragging a process task onto a managed system or systems.

**public key.** A central component of the digital-signature algorithm. Each managed system holds a public key that corresponds to the private key held by

the management server. When the management server requests access, the managed system sends the management server the public key and a random data block. The management server then generates a digital signature of the data block using its private key and sends it back to the managed system. The managed system then uses the public key to verify the validity of the signature.

## R

**Rack Manager task.** An IBM Director extension available in the Server Plus Pack that can be used to group equipment in virtual racks by associating equipment such as managed systems and devices, networking devices, power devices, and monitors with a rack to visually represent an existing rack in a network environment.

**RDM.** See Remote Deployment Manager.

**Real Time Diagnostics.** An IBM Director extension that you can use to run industry-standard diagnostic utilities on servers while they are running.

**redirected distribution.** A method of software distribution that uses a file-distribution server.

**Remote Control task.** An IBM Director task that can be used to manage a remote system by displaying the screen image of the managed system on a management console.

**Remote Deployment Manager (RDM).** An extension to IBM Director that handles deployment and configuration of IBM systems. Using RDM, a network administrator can remotely flash BIOS, modify configuration settings, perform automated installations of operating systems, back up and recover primary partitions, and permanently erase data when systems are redeployed or retired.

**remote I/O enclosure.** An IBM Director managed object that represents an expansion enclosure of PCI-X slots, for example, an RXE-100 Remote Expansion Enclosure. The enclosure consists of one or two expansion kits. Each expansion kit contains six hot-swap Active PCI-X adapter slots.

**Remote Session task.** An IBM Director task that can be used to run command-line programs on a remote managed system. Remote Session uses less network traffic and system resources than the Remote Control task and, therefore, is useful in low-bandwidth situations.

**Remote Supervisor Adapter.** An IBM service processor. It is built into the system board of some xSeries servers and available as an optional adapter for use with others. When used as a gateway service

processor, the Remote Supervisor Adapter can communicate with all service processors on the ASM interconnect.

**Resource Monitors task.** An IBM Director task that can be used to provide statistics about critical system resources, such as microprocessor, disk, and memory usage. It is used to set thresholds to detect potential problems with managed systems or devices. When a threshold is met or exceeded, an event is generated.

**resource-monitor threshold.** The point at which a resource monitor generates an event.

**RXE Expansion Port.** The dedicated high-speed port used to connect a remote I/O expansion unit, such as the RXE-100 Remote Expansion Enclosure, to a server.

## S

**scalable node.** A physical platform that has at least one SMP Expansion Module. Additional attributes are assigned to a physical platform when it is a scalable node. These additional attributes record the number of SMP Expansion Modules, SMP Expansion Ports, and RXE Expansion ports on the physical chassis.

**scalable object.** An IBM Director managed object that is used with Scalable Systems Manager. Scalable objects include scalable nodes, scalable systems, scalable partitions, and remote I/O enclosures that are attached to scalable nodes.

**scalable partition.** An IBM Director managed object that defines the scalable nodes that can run a single image of the operating system. A scalable partition has a single, continuous memory space and access to all associated adapters. A scalable partition is the logical equivalent of a physical platform. When Scalable Systems Manager is installed, you can power-on and power-off a supported scalable partition through IBM Director Console. IBM Director manages a scalable partition through the service processor on the primary scalable node of that scalable partition. Scalable partitions are associated with scalable systems and comprise only the scalable nodes from their associated scalable systems.

**scalable system.** An IBM Director managed object that consists of scalable nodes and the scalable partitions that are made from the scalable nodes in the scalable system. When a scalable system contains two or more scalable nodes, the servers that they represent must be interconnected through their SMP Expansion Modules to make a multinode configuration, for example, a 16-way xSeries 455 server made from four scalable nodes. When a scalable node is unlocked, IBM Director automatically creates a scalable system and scalable partition containing that scalable node based on the information stored in NVRAM of the service processor.

**Scheduler.** An IBM Director function that executes a single noninteractive task or set of noninteractive tasks at a specific date and time or in a repeating interval.

**secure sockets layer (SSL).** A security protocol developed by Netscape. Designed to enable secure data transmission on a unsecure network, it provides encryption and authentication using digital certificates such as those provided by the digital-signature algorithm. In the IBM Director environment, it can be used to secure communications between the management server and management console.

**Server Plus Pack.** See IBM Director Server Plus Pack.

**ServeRAID Manager task.** An IBM Director task that can be used to monitor ServeRAID controllers that are installed locally or remotely on servers. In IBM Director, you can use the ServeRAID Manager task to view information related to arrays, logical drives, hot-spare drives, and physical drives and view configuration settings. You also can view alerts and locate defunct disk drives.

**Service Location Protocol (SLP).** A protocol developed by the Internet Engineering Task Force (IETF) to discover the location of services on a network automatically. It is used by IBM Director Server to discover BladeCenter chassis and multi-node servers such as the xSeries 445 and xSeries 455 servers.

**service processor.** A generic term for Remote Supervisor Adapters, Advanced System Management processors, Advanced System Management PCI adapters, and integrated system management processors. These hardware-based management processors used in IBM Netfinity and xSeries servers work with IBM Director to provide hardware status and alert notification.

**Slot Manager.** An Active PCI Manager subtask that can be used to display information about all PCI and PCI-X adapters, analyze PCI and PCI-X performance, and determine the best slots in which to install PCI and PCI-X adapters in a managed system.

**SLP.** See service location protocol.

**SMBIOS.** See systems management BIOS.

**SMP Expansion Cable.** The cable used to connect two SMP Expansion Ports.

**SMP Expansion Module.** An IBM xSeries hardware option. It is a single module that contains microprocessors, disk cache, random access memory, and three SMP Expansion Port connections. Two SMP Expansion Modules can fit in a chassis. The IBM xSeries 440 server is the first hardware platform that uses SMP Expansion Modules.

**SMP Expansion Port.** A dedicated high-speed port used to interconnect SMP Expansion Modules.

**SNMP Access and Trap Forwarding.** An IBM Director Agent feature that enables SNMP as a protocol for accessing managed-system data. When installed on a managed system, this feature enables SNMP-based managers to poll the managed system and receive its alerts. If System Health Monitoring is installed on the managed system also, hardware alerts can be forwarded as SNMP traps.

**SNMP Browser task.** An IBM Director task that can be used to view and configure the attributes of SNMP devices, for example, hubs, routers, or other SNMP-compliant management devices. You also can use it for SNMP-based management, troubleshooting problems, or monitoring the performance of SNMP devices.

**SNMP device.** A network device, printer, or computer that has an SNMP device installed or embedded.

**SNMP discovery.** See discovery, SNMP.

**Software Distribution task.** An IBM Director task that can be used to import and distribute software packages to an IBM Director managed system or systems. To use the full-featured Software Distribution task (Premium Edition), you must purchase and install the IBM Director Software Distribution (Premium Edition).

**Software Rejuvenation task.** An IBM Director extension available in the Server Plus Pack that can be used to schedule the restart of managed systems or services and configure predictive rejuvenation, which monitors resource utilization and rejuvenates managed systems automatically before utilization becomes critical.

**SSL.** See secure sockets layer.

**SSM.** See Scalable Systems Manager.

**static group.** See group, static.

**static partition.** A view-only scalable partition.

**switch module.** The BladeCenter component that provides network connectivity for the BladeCenter chassis and blade servers. It also provides interconnectivity between the management module and blade servers.

**system.** A desktop computer, workstation, server, or mobile computer.

**System Availability task.** An IBM Director extension available in the Server Plus Pack that can be used to analyze the availability of a managed system or group and display statistics about managed system uptime and downtime through reports and graphical representations. It also can identify problematic

managed systems that have had too many unplanned outages over a specified period of time.

**System Health Monitoring.** An IBM Director Agent feature that provides active monitoring of critical system functions, including system temperatures, voltages, and fan speeds. It also handles in-band alert notification for managed systems running Windows and some managed systems running Linux.

**system variable.** A user-defined keyword and value pair that can be used to test and track the status of network resources. System variables can be referred to wherever event-data substitution is allowed.

**systems management BIOS (SMBIOS).** A key requirement of the WfM 2.0 specification. SMBIOS extends the system BIOS to support the retrieval of management data required by the WfM specification. To run IBM Director Agent, a system must support SMBIOS, version 2.2 or later.

## T

**target system.** A managed system on which an IBM Director task is performed.

**task-based group.** See group, task-based.

**time to live (TTL).** The number of times a multicast discovery request is passed between subnets. When the TTL is exceeded, the packet is discarded.

**triple data encryption standard (DES).** A block cipher algorithm that can be used to encrypt data transmitted between managed systems and the management server. This is a security enhancement of DES that employs three successive DES block operations.

**TTL.** See time to live.

## U

**unicast discovery.** See discovery, unicast.

**universal unique identifier (UUID).** A 128-bit character string guaranteed to be globally unique and used to identify components under management. The UUID enables inventory-level functionality and event tracking of scalable nodes, scalable partitions, scalable systems, and remote I/O enclosures.

**Update Assistant.** A wizard that can be used to import IBM software and create software packages. It is part of the Software Distribution task.

**upward integration.** The methods, processes and procedures that enable lower-level systems-management software, such as IBM Director Agent, to work with higher-level systems-management software, such as Tivoli Enterprise™ or Microsoft SMS.

**upward integration module.** Software that enables higher-level systems-management software, such as Tivoli Enterprise or Microsoft Systems Manager Server (SMS), to interpret and display data provided by IBM Director Agent. A module also can provide enhancements that you can use to start IBM Director Agent from within the higher-level systems-management console, as well as collect IBM Director inventory data and view IBM Director alerts.

**UUID.** See universal unique identifier.

## V

**vital product data (VPD).** The key information about a server, its components, POST/BIOS, and service processor. This includes machine type, model numbers, component FRU number, serial number, manufacturer ID, and slot numbers; POST/BIOS version number, build level, and build date; and service processor build ID, revision numbers, file name, and release date.

**VPD.** See vital product data.

## W

**Wake on LAN.** A technology that enables you to remotely turn on systems for off-hours maintenance. A result of the Intel-IBM Advanced Manageability Alliance and part of the Wired for Management Baseline Specification, this technology enables you to remotely turn on a server. After the server is started, it can be controlled across the network, thus saving time on automated software installations, upgrades, disk backups, and virus scans.

**Web-based Access.** An IBM Director Agent feature that, when installed on a managed system running Windows, enables you to use a Web browser or Microsoft Management Console (MMC) to view real-time asset and health information about the managed system.



---

# Index

## A

- abbreviations 241
- Active PCI Manager
  - hardware, supported 8
  - managed systems, installing on 131
  - management console, installing on 60
  - management server, installing on 47
  - operating systems, supported 17
  - overview 8
  - prerequisites 134
  - subtasks 8
  - troubleshooting 143, 221
- Add BladeCenter Chassis window 115
- Add Management Processors window 96
- Add Physical Platforms window 213
- admin4.txt file 105
- Advanced Systems Management PCI adapter
  - See ASM PCI adapter
- Advanced Systems Management processor
  - See ASM processor
- Agent
  - See IBM Director Agent
- AIX installation
  - IBM Director Agent 65
  - uninstalling 204
  - Wake on LAN, enabling 197
- Alert-forwarding profiles, troubleshooting 210, 222
- alert-forwarding strategy, service processors 26
- alerts
  - ISMP and limitations 23
  - MPA Agent, role of 23
  - out-of-band 24
  - remote login 211
  - System Health Monitoring, role of 23
- Apache Web Server, troubleshooting 226
- ASM interconnect gateway
  - gateway service processors 23
  - ISMPs, enabling communication with 23
- ASM interconnect network
  - ASM PCI adapter 25
  - ASM processor 25
  - configuring 22
  - definition 23
  - gateway service processor, role of 23
  - ISMP 25
  - Remote Supervisor Adapter 25
- ASM PCI adapter
  - alert-forwarding strategies 26
  - ASM interconnect network 25
  - configuring 96
  - Management Processor Assistant Agent 6
  - management processor object, creating 96
  - out-of-band communication, pathways for 26
  - use as a gateway service processor 23
- ASM processor
  - alert-forwarding strategies 26
  - ASM interconnect network 25

- ASM processor (*continued*)
  - Management Processor Assistant Agent 6
  - out-of-band communication, pathways for 26
  - out-of-band management 96
- Asset ID, troubleshooting 223
- attention notice xiv

## B

- BIOS code, updating 21, 22
- blade servers
  - boot sequence 117
  - deployment policies 117
  - installing operating systems 128
- BladeCenter
  - chassis
    - assigning IP addresses manually 114, 115
    - configuring 117
    - DHCP server, using 114
    - discovering (automatically) 114
    - discovering (manually) 114
    - IP address conflicts 113
    - managed object 114
  - deployment infrastructure
    - changing IBM Director database 113
    - DHCP server, using 27, 113
    - illustration 27
    - IP address conflicts 27, 113
    - multiple NICs 212
    - security 27
  - documentation xv
  - management module
    - assigning temporary IP addresses 27
    - IP address (default) 27
    - user name and password (default) 115
  - troubleshooting 212, 215
- BladeCenter Assistant, troubleshooting 221
- BladeCenter Deployment wizard
  - chassis detect-and-deploy profile
    - creating 117, 129
    - overwriting 129
  - configuring the chassis 117
  - deployment policies 117
  - IP settings, configuring 124
  - management module
    - logging in to 120
    - network protocols, configuring 123
    - properties, configuring 122
  - operating systems, deploying 128
- profiles
  - changing name of 129
  - displayed in IBM Director Console (screenshot) 130
  - overview 117
- switch modules
  - external ports, configuring 126
  - network protocols, configuring 126
  - user name and password, changing 125

- books xiv
- broadcast discovery 94
- broadcast relay 94

## C

- Capacity Manager
  - managed systems, installing on 131
  - management console, installing on 60
  - management server, installing on 47
  - overview 8
  - supported operating systems 17
- CCSID 5026, troubleshooting 214
- cfgdb utility, troubleshooting 212, 215
- chassis (BladeCenter)
  - configuring 117
  - DHCP server, using 114
  - discovering (automatically) 114
  - discovering (manually) 114
  - IP address conflicts 113
  - managed object 114
  - manually assigning IP addresses 114, 115
- chassis detect-and-deploy profile
  - creating 117
  - definition 117
  - overwriting 129
- chassis managed objects
  - creating 114
  - displayed in IBM Director Console (screenshot) 114
  - troubleshooting 117
- Chinese characters incorrectly displayed 226
- Chinese-language systems, troubleshooting 227
- CIM Browser, troubleshooting 221
- Cluster Systems Management 10
- compatibility documents xvi, 11
- computer name displayed incorrectly 223
- Console
  - See IBM Director Console
- customer support xv

## D

- dacimom startup script 199
- daemon.stderr file 214, 219
- data directory, location of 103
- Data Encryption Standard
  - See DES
- data space, troubleshooting 223
- data values, troubleshooting 220
- database
  - configuration, troubleshooting 212, 215
  - DB2 Universal Database
    - Linux installation 29
    - Windows installation 30
  - function of 5
  - initialization error 212
  - installing after IBM Director Server is installed 203
  - Microsoft Data Engine 1.0 30
  - Microsoft Jet 4.0
    - overview 30
    - size limitations 30

- database (*continued*)
  - Microsoft SQL Server 31
  - Oracle Server
    - JDBC driver 31
    - overview 31
  - PostgreSQL 32
  - selecting 21, 22
  - SQL Server 2000 Desktop Engine 30
  - supported applications 28
  - troubleshooting
    - cfgdb utility 212
    - Oracle Server 212
- database applications, supported 28
- DB2 Universal Database
  - Linux installation 29
  - Windows installation 30
- DBCS languages, troubleshooting 227
- default router, setting 213, 218
- definitions
  - ASM interconnect network 23
  - chassis detect-and-deploy profile 117
  - extensions 7
  - gateway service processor 23
  - in-band communication 22
  - interprocess communication 22
  - managed system 3
  - management console 4
  - management server 3
  - out-of-band communication 22
  - service account 32
  - SNMP device 3
- deployment infrastructure (BladeCenter)
  - changing IBM Director database 113
  - DHCP server, using 27, 113
  - illustration 27
  - IP address conflicts 27, 113
  - security 27
- deployment policies 117
- DES 34
- detect-and-deploy profile
  - creating 117
  - overwriting 129
- device driver
  - LM78 (Linux) 63
  - Remote Supervisor Adapter II 222
  - SMBus (Linux) 63
  - SMBus, detection of (Windows) 209, 214, 219
- device drivers, updating 21, 22
- DHCP server 113, 114
- Diffie-Hellman key exchange 34
- Digital Signature Algorithm 233
- DirAdmin 33, 97
- diragent.rsp file
  - customizing 77, 182, 188
  - location 77, 182, 188
  - upgrading IBM Director Agent using Software Distribution 190
- dircon.rsp file
  - customizing 62, 167
  - location 61, 166

- dirinstall script
  - IBM Director Agent 67, 173
  - IBM Director Console 57, 161
  - IBM Director Server 42, 150
  - upgrading IBM Director Agent using Software Distribution 190
- dirinstall script, location of 199
- dirsnmpd startup script 199
- DirSuper 33, 97
- diruninstall script 205
- diruns utility 207
- DirWbs service 210, 211
- discovery
  - See ding network
  - BladeCenter chassis 113
  - broadcast 94
  - broadcast relay 94
  - default router, setting 213, 218
  - multicast 94
  - overview 93
  - physical platforms 213
  - RXE-100 213
  - service processors 95
  - setting preferences 95
  - troubleshooting 212, 213
  - unicast 94
- Discovery Preferences window 213
- discovery preferences, setting 95
- disk space, troubleshooting 221
- display requirements 209
- distorted characters, troubleshooting 222
- Distribution Preferences window, troubleshooting 225
- documentation
  - Digital Certificate Manager 103
  - IBM Director xiv
  - Redbooks xv
  - service processors xv
  - Virtualization Engine 41
- domain controller 21
- downloading xvi
  - compatibility documents xvi
  - hardware compatibility information xvi
  - IBM Director code xvi
  - IBM Director publications xvi
  - LM78 device driver 64
  - management module firmware 28
  - Net-SNMP, version 5.09 198
  - SMBus device driver 64
  - systems-management software xvi
  - wmint4.exe 71
- dynamic groups criteria, troubleshooting 216

## E

- eFixes
  - See interim fixes
- Electronic Service Agent 10
- encryption
  - algorithms 34
  - enabling on managed system
    - AIX 65

- encryption (*continued*)
  - enabling on managed system (*continued*)
    - Linux 67
    - OS/400 66
    - Windows 74
  - enabling on management server
    - i5/OS 41
    - Linux 43
    - Windows 49
  - overview 34
  - performance penalty 34
  - troubleshooting 213, 218
- environment
  - illustration 4
  - ports used 19
  - reviewing 21
- error message
  - an IO error occurred 218
  - event ID 2003 221
  - exception in thread "main" 219
  - IRQL\_NOT\_LESS\_OR\_EQUAL 210
  - Windows error 1306 210
  - Windows error 1722 209
  - Windows error 1921 210
- eServer Information Center xvi
- Event Action Plan wizard
  - access to, restricting 99, 102
  - event action plan, applying 92
  - event action plan, naming 93
  - event filters, selecting 89
  - event substitution variables, using 91
  - notification method, selecting 90
  - systems and devices, discovering 93
- event action plans
  - displayed in IBM Director Console 216
  - troubleshooting 214, 216
- event actions, troubleshooting 214
- event log
  - full 220
  - troubleshooting 209, 214, 219
- events
  - filtering, troubleshooting 210
  - selecting filters 89
  - substitution variables 91
- extensions
  - Cluster Systems Management 10
  - Electronic Service Agent 10
  - Real Time Diagnostics 10
  - Remote Deployment Manager 9
  - Scalable Systems Manager 10
  - Server Plus Pack 8
  - Software Distribution (Premium Edition) 9
  - Virtual Machine Manager 10
- extensions, definition 7

## F

- Fault Tolerant Management Interface
  - overview 8
  - prerequisites 134
- File Distribution Servers Manager window 224

- file-distribution server
  - configuring 108
  - considerations 107
  - setting up 107
  - troubleshooting 225
- filtering events, troubleshooting 210
- firewall access
  - configuring 19
  - troubleshooting 223, 224
- firmware, updating 21, 22
- FRU information, troubleshooting 222
- FTP share, troubleshooting (i5/OS) 225

## G

- gateway service processor, definition 23
- GETFRU command 222
- glossary 249

## H

- hardware compatibility xvi
- hardware requirements 13
- help files, Web-based Access 7
- help, IBM Director resources xv

## I

- i5/OS installation
  - documentation 41
  - encryption, enabling 41, 66
  - IBM Director Agent, installing 66
  - IBM Director Server, installing 41
  - software distribution, troubleshooting 225
  - starting 66
  - troubleshooting 214
- IBM Active PCI Software for Microsoft Windows 134
- IBM Active PCI Software for SUSE LINUX Enterprise Server 8 134
- IBM Director Agent
  - AIX, installing on
    - encryption, enabling 65
    - prerequisites 65
    - WAKE on LAN, enabling 66
  - encryption, enabling
    - AIX 65
    - Linux 67, 173
    - OS/400 66
    - Windows 74
  - function 5
  - hardware requirements 13
  - imaging, troubleshooting 217
  - license 6, 11
  - Linux, installing on
    - dirinstall script 67, 173
    - Net-SMNP, enabling 68
    - Wake on LAN, enabling 68
  - modifying an installation
    - AIX 197
    - Linux 197
    - NetWare 201

- IBM Director Agent (*continued*)
  - modifying an installation (*continued*)
    - troubleshooting 209
    - Windows 203
  - NetWare, installing on
    - features, selecting 69
    - network driver, configuring 70
  - network protocols 18
  - operating systems, supported 15
  - troubleshooting
    - installing 209, 210
    - starting 209, 219
    - upgrading 210
  - uninstalling
    - i5/OS 205
    - Linux 205
    - NetWare 206
    - troubleshooting 211
    - Windows 206
  - upgrading
    - Linux 172
    - NetWare 174
    - Software Distribution task, using 189
  - upgrading on Windows
    - diragent.rsp file 182, 188
    - encryption, enabling 178, 185
    - features, selecting 177, 184
    - InstallShield wizard, using 176, 183
    - network driver, configuring 181, 187
    - securing managed system 178, 185
    - security state, setting 178, 185
    - software-distribution settings 179, 186
    - unattended installation, using 182, 188
    - Wake on LAN, enabling 181, 187
  - Windows, installing on
    - diragent.rsp file 77
    - encryption, enabling 74
    - features, selecting 72, 79
    - InstallShield wizard, using 71
    - network driver, configuring 76, 81
    - securing managed system 74
    - security state, setting 74
    - software-distribution settings 74
    - unattended installation, using 77
    - Wake on LAN, enabling 76, 82
- IBM Director Agent features
  - Management Processor Assistant Agent 6
  - Remote Control Agent 7
  - ServeRAID Manager 6
  - SNMP Access and Trap Forwarding 7
  - Web-based Access help files 7
- IBM Director Agent Web Server (DirWbs) service 210, 211
- IBM Director Agent.msi file 209
- IBM Director Console
  - display requirements 209
  - features, selecting 59
  - function 6
  - hardware requirements 13
  - installing on Linux 57

- IBM Director Console *(continued)*
  - installing on Windows
    - dircon.rsp file 61
    - InstallShield wizard, using 58
    - Server Plus Pack 60
    - unattended mode, using 61
  - license 6, 11
  - modifying an installation
    - Linux 197
    - troubleshooting 209
    - Windows 203
  - network protocols 18
  - screenshot 88
  - starting 87
  - supported operating systems 16
  - troubleshooting
    - BladeCenter 215
    - data displayed in windows 215
    - deleted physical platform object displayed 215
    - discovered systems not displayed 213, 218
    - logon failure 219
    - managed system access denied 217, 219
    - managed system icon with question mark 216
    - managed systems not displayed 217
    - starting 218
    - time zone error 219
  - uninstalling
    - Linux 205
    - Windows 206
  - upgrading on Linux 161
  - upgrading on Windows
    - dircon.rsp file 166
    - features, selecting 165
    - InstallShield wizard, using 163
    - unattended mode, using 166
- IBM Director Console.msi 209
- IBM Director Hardware and Software Compatibility
  - document xvi
- IBM Director Multiplatform
  - documentation xvi
  - overview 3
- IBM Director Server
  - configuration data 204
  - determining if running 215
  - encryption, enabling
    - i5/OS 41
    - Linux 43
    - troubleshooting 214
    - Windows 49
  - function 5
  - hardware requirements 13
  - i5/OS, installing on 41
  - license 5, 11
  - Linux, installing on
    - database, configuring 43
    - encryption, enabling 151
  - modifying an installation
    - Linux 197
    - Windows 203
  - network protocols 18
  - service processors, communication with 22
- IBM Director Server *(continued)*
  - SSL enabled, troubleshooting 214
  - supported operating systems 15
  - troubleshooting
    - database 212
    - event log error 221
    - installing 209
    - Microsoft Jet 211
    - starting 209, 214
    - Telnet 212
  - uninstalling
    - i5/OS 205
    - Linux 205
    - Windows 206
  - upgrading on Linux 150
  - upgrading on Windows
    - encryption settings 157
    - features, selecting 155
    - network driver, configuring 159
    - Server Plus Pack 155
    - software-distribution settings 158
    - Wake on LAN, enabling 159
  - where to install 21
  - Windows, installing on
    - database configuration 52
    - encryption settings 49
    - features, selecting 46
    - network driver, configuring 51
    - Server Plus Pack 47
    - service account 44
    - Software Distribution settings 50
    - Wake on LAN, enabling 51
- IBM Director Support Program service (TWGIPC) 210, 211
- IBM LM78 device driver for Linux 63
- IBM SMBus device driver for Linux 63
- IBM systems-management software
  - downloading xvi
  - overview xv
- IBM Web sites
  - eServer Information Center xvi
  - iSeries Information Center 214
  - Redbooks xv
  - ServerProven xvi
  - Support xvi
  - Systems Management Software xvi
  - xSeries Systems Management xvi
- identifying service processors 22
- illustrations
  - BladeCenter deployment infrastructure 27
  - Director software components 5
  - IBM Director environment 4
- imaging IBM Director Agent, troubleshooting 217
- important notice xiv
- in-band communication 23
  - definition 22
  - enabling 23
  - ISMPs, limitations 23
  - MPA Agent, role of 23
- installation, troubleshooting 209

- InstallShield wizard
  - IBM Director Agent 71
  - IBM Director Console 58
  - IBM Director Server 44
- insufficient data space, troubleshooting 223
- insufficient disk space, troubleshooting 221
- insufficient memory, troubleshooting 216
- integrated systems management processor
  - See ISMP
- interim fixes xv
- interprocess communication, definition 22
- invalid data values, troubleshooting 220
- inventory errors, troubleshooting 113, 222
- Inventory task, troubleshooting 220, 222
- IP address conflicts, troubleshooting 113
- IPMI baseboard management controller
  - MPA Agent 6
- iSeries Information Center 214
- ISMP
  - alert-forwarding strategies 26
  - ASM interconnect network 25
  - limitations on in-band communication 23
  - MPA Agent 6
  - out-of-band communication, pathways for 26

## J

- Japanese-language systems, troubleshooting 225, 227
- JDBC driver, Oracle Server 31
- JRE exceptions, troubleshooting 216
- JVM, troubleshooting 226

## K

- keys
  - files, location of 234
  - origin of, determining 238
  - recovering lost keys 239
- Korean-language systems, troubleshooting 225, 227

## L

- license
  - IBM Director Agent 6, 11
  - IBM Director Console 6, 11
  - IBM Director Server 5, 11
- Linux device drivers 22
- Linux installation
  - encryption, enabling 43, 67, 173
  - IBM Director Agent 66, 172
  - IBM Director Console 57, 161
  - IBM Director Server 42, 150
  - LM78 device driver 63
  - modifying
    - adding a feature 199
    - installing the IBM Director database 197
    - removing a feature 200
    - SNMP Access and Trap Forwarding, enabling 198
    - Wake on LAN, enabling 198
  - Rack Manager installation, completing 131

- Linux installation (*continued*)
  - Server Plus Pack extensions 135
  - SMBus device driver 63
  - starting 68
  - stopping 200
  - uninstalling 205
- LM78 device driver
  - downloading 64
  - installing 65
- LM78 device driver for Linux 63
- locked files, troubleshooting 211
- locked files, Web-based Access 211
- logical disk drives, troubleshooting 221

## M

- managed objects, creating
  - BladeCenter chassis 115
  - management processor 22, 96
- managed systems
  - access request denied 217, 219
  - behind firewall, troubleshooting 223, 224
  - definition 3
  - distribution preferences, configuring 110
  - firewall access 222
  - hardware requirements 13
  - installing the Server Plus Pack
    - manually 135
    - using Software Distribution task 138
  - invalid data values 220
  - running Windows, troubleshooting 220
  - securing
    - automatically 235
    - IBM Director Agent installation, during 74
    - IBM Director Agent upgrade, during 178, 185
    - manually 236
    - methods 235
  - security 237
  - troubleshooting
    - encryption 213, 218
    - resource-monitor information 220
    - time zone error 219
- management console
  - definition 4
  - hardware requirements 13
  - insufficient disk space 224
  - troubleshooting 215
- management module
  - assigning temporary IP addresses 27
  - firmware, upgrading 28
  - IP address (default) 27
  - logging in to 120
  - network protocols, configuring 123
  - properties, configuring 122
  - user name and password (default) 115
- Management Module Network Interfaces window 116
- Management Processor Assistant Agent
  - managed system, installing on 70, 72
  - management server, installing on 46
  - NetWare, installing on 68
  - overview 6

- Management Processor Assistant task
  - distorted characters, troubleshooting 222
  - overview 6
  - troubleshooting 210, 222, 227
- management processor object
  - creating 22, 96
  - displayed in IBM Director Console (screenshot) 97
  - naming 96
- management server
  - DB2 database
    - Linux installation 29
    - Windows installation 30
  - definition 3
  - hardware requirements 13
  - logon failure 219
  - Rack Manager installation, completing 131
  - Software Distribution, installing
    - i5/OS 132
    - Linux 133
    - Windows 133
  - troubleshooting 211
- managing systems running IBM Director Agent 3.1 11
- Mass Configuration task, troubleshooting 223
- memory, troubleshooting 216
- message digest 5 method, troubleshooting 217, 219
- MIB file attribute values, troubleshooting 223, 224
- Microsoft Data Engine 1.0 30
- Microsoft Internet Explorer, troubleshooting 226
- Microsoft Jet 4.0
  - overview 30
  - size limitations 30
- Microsoft Knowledge Base Article
  - 259403 71
  - 267831 221
  - 825236 210
  - 827439 220
  - 830459 220
- Microsoft Management Console 7, 20
- Microsoft Run-Time Components for Visual C++ Applications 71
- Microsoft SQL Server 31
- Microsoft Windows 2000 Service Pack 4 220, 221
- modifying an IBM Director installation
  - Linux installation
    - adding a feature 199
    - installing the IBM Director database 197
    - removing a feature 200
    - SNMP Access and Trap Forwarding, enabling 198
    - Wake on LAN, enabling 198
  - NetWare installation
    - adding a feature 201
    - limitations 201
  - Windows installation
    - adding a feature 203
    - installing the IBM Director database 203
    - Program Maintenance window 204
    - removing a feature 203
- MPA
  - See Management Processor Assistant
- multicast discovery 94

- multiple NICs, troubleshooting 212

## N

- Net-SNMP, version 5.0.9 198
- Netscape Navigator, troubleshooting 226, 227
- NetWare installation
  - IBM Director Agent, installing 68
  - modifying
    - adding a feature 201
    - limitations 201
  - MPA Agent, when to install 68
  - Server Plus Pack extensions 136
  - uninstalling 206
- network adapter attribute names, troubleshooting 223
- Network Configuration task, troubleshooting 223
- network protocols 18
- network share, troubleshooting 224
- network timeout value, modifying 217
- New Scheduled Job window 143, 194
- non-English language keyboard, troubleshooting 223
- notices
  - attention xiv
  - important xiv
  - notes xiv

## O

- operating system compatibility xiv
- operating systems, supported 14
- optional service processors, configuring 22
- Oracle Server
  - JDBC driver 31
  - overview 31
  - troubleshooting 212
- Oracle TCP/IP listener 212
- OS/400
  - See i5/OS
- out-of-band communication
  - ASM PCI adapter 26
  - ASM processor 26
  - definition 22
  - ISMP 26
  - Remote Supervisor Adapter 26
  - SSM 23

## P

- PCI adapter, troubleshooting 221
- physical platforms, discovery of 213
- planning considerations 21
- platform managed object 215
- policies, deployment 117
- ports 19
- PostgreSQL
  - JDBC driver 32
  - overview 32
- problem solving 209
- profiles (BladeCenter Deployment wizard)
  - changing name of 129
  - displayed in IBM Director Console (screenshot) 130

profiles (BladeCenter Deployment wizard) *(continued)*  
overview 117  
publications xiv

## R

Rack Manager  
completing installation on management server  
Linux 131  
Windows 132  
management console, installing on 60  
management server, installing on 47  
overview 9  
supported operating systems 17  
RAID arrays, monitoring and managing 6  
Real Time Diagnostics 10  
Redbooks xv  
redirector share, troubleshooting 224  
Remote Access Connection Manager service,  
troubleshooting 220  
Remote Control Agent  
managed system, installing on 72  
management server, installing on 46  
overview 7  
Remote Control task, troubleshooting 223  
Remote Deployment Manager  
BladeCenter deployment infrastructure 28  
overview 9  
Remote Supervisor Adapter  
alert-forwarding strategies 26  
ASM interconnect network 25  
configuring 96  
documentation xv  
firmware levels 26  
Management Processor Assistant 6  
management processor object, creating 96  
out-of-band communication, pathways for 26  
use as an ASM interconnect gateway 23  
Remote Supervisor Adapter II  
device driver 222  
troubleshooting 222  
Resource Monitors task, troubleshooting 223  
resource-monitor information, troubleshooting 220  
response files  
See diragent.rsp file, dircon.rsp file, and dirinstall  
script  
RPM packages, troubleshooting 220, 222  
RS-485 ports 23  
RXE-100 Remote Expansion Enclosures  
configuring using SSM 10  
use with xSeries 360 or 440 servers 25

## S

salt values, required lengths 217, 219  
Scalable Systems Manager  
See SSM  
screenshots  
BladeCenter Deployment wizard profile 130  
IBM Director Console 88  
management processor object 97

screenshots *(continued)*  
software packages 142  
secure sockets layer  
cipher suites 34  
enabling 103  
overview 34  
restricting sessions 104  
security  
BladeCenter deployment infrastructure 27  
Digital Signature Algorithm 233  
encryption  
algorithms 34  
performance penalty 35  
IBM Director Agent-Server authentication 233  
key management  
location of files 234  
origin of a key, determining 238  
public and private keys 234  
recovering lost keys 239  
managed system  
accessing a secured system 237  
removing access to 237  
securing automatically 235  
securing manually 236  
management server, adding another 238  
overview 32  
secure sockets layer  
cipher suites 34  
enabling 103  
overview 34  
restricting sessions 104  
user administration  
default profile, creating 97  
editing user privileges 99  
Event Action Plan wizard, restricting access  
to 99, 102  
group access, restricting 101  
task access, restricting 102  
user login 97  
Web-based Access  
custom access policy, configuring 105  
overview 35  
Server  
See IBM Director Server  
Server Plus Pack  
installation 8  
managed systems, installing on  
manually 135  
using Software Distribution task 138  
operating systems, supported 17  
overview 8  
purchasing 8  
Server Preferences window 220, 222  
server.xml file 226  
ServeRAID inventory missing 222  
ServeRAID Manager 6  
managed system, installing on 70, 72, 79  
management console, installing on 60  
management server, installing on 46  
overview 6

- service account
  - creating 32
  - definition 32
- Service Location Protocol 114
- service packs xv
- service processors
  - See also* ASM processor, ASM PCI Adapter, ISMP, and Remote Supervisor Adapter
  - alert-forwarding strategies 26
  - ASM interconnect 24
  - communicating with IBM Director Server
    - in-band 6
    - interprocess communication 22
    - out-of-band 24
    - over the ASM interconnect 22
    - over the LAN 22
  - communication with IBM Director Server 22
  - configuring 22
  - discovery of 95
  - documentation xv
  - identifying 22
  - in-band communication
    - MPA Agent, role of 23
    - operating system 23
    - service processor type 23
  - management processor object, creating 96
  - managing 6
- ServiceNodeLocal.properties file 217
- session support, disabling 223, 224
- silent installations
  - See* unattended installations
- silent parameter 62, 78, 83
- Simplified-Chinese systems, troubleshooting 227
- Slot Manager
  - overview 8
  - troubleshooting 143
- SMBIOS 13
- SMBus device driver
  - downloading 64
  - installing 65
- SMBus device driver for Linux 63
- SNMP Access and Trap Forwarding
  - enabling on Linux 198
  - managed system, installing on 72
  - management server, installing on 46
  - overview 7
- SNMP agents 213
- SNMP device
  - definition 3
  - troubleshooting 213, 223, 224
- SNMP service 213
- SNMP traps
  - enabling 21
  - troubleshooting 224
- snmpconf utility 198
- snmpd.conf file 199
- software components (illustration) 5
- software distribution
  - methods
    - redirected distribution 106
    - streaming from management server 106
  - software distribution (*continued*)
    - overview 106
    - preferences, configuring 109
    - Server Plus Pack, installing
      - creating a software package 138
      - installing a software package 142
      - overview 138
      - XML files, location of 138
    - upgrading IBM Director Agent
      - overview 189
      - software package, installing 194
  - Software Distribution (Premium Edition)
    - installing on the management server
      - i5/OS 132
      - Linux 133
      - Windows 133
    - overview 9, 106
    - troubleshooting 225
  - Software Distribution task, troubleshooting
    - file-distribution server 225
    - managed system behind firewall 224
    - package creation 224
  - software packages
    - creating 190
    - displayed in IBM Director Console (screenshot) 142, 193
    - SPB format, troubleshooting 225
  - Software Rejuvenation
    - managed systems, installing on 131
    - management console, installing on 60
    - management server, installing on 47
    - overview 9
    - supported operating systems 17
  - solving problems 209
  - SQL Server 2000 Desktop Engine 30
  - SSM (Scalable Systems Manager)
    - IP addresses 23
    - out-of-band communication 23
    - overview 10
  - substitution variables 91
  - switch modules
    - external ports, configuring 126
    - network protocols, configuring 126
    - user name and password, changing 125
- System Availability
  - managed systems, installing on 131
  - management console, installing on 60
  - management server, installing on 47
  - overview 9
  - supported operating systems 17
- System Health Monitoring
  - managed system, installing on 72
  - support for Linux systems 24
  - uninstalling 203

## T

- task bar icons (Windows) 215, 218
- tcpip.ini file 223, 224
- terminology
  - ASM interconnect network 23

- terminology (*continued*)
  - chassis detect-and-deploy profile 117
  - extensions 7
  - gateway service processor 23
  - in-band communication 22
  - interprocess communication 22
  - managed system 3
  - management console 4
  - management server 3
  - out-of-band communication 22
  - service account 32
  - SNMP device 3
- terminology, summary 241
- timeout, troubleshooting 214
- tomcat.conf file 226
- trademarks 248
- Traditional-Chinese systems, troubleshooting 227
- Triple DES 34
- troubleshooting
  - Active PCI Manager 221
  - Asset ID 223
  - BladeCenter discovery 212
  - CCSID 5026 214
  - cfgdb utility 212
  - Chinese characters incorrectly displayed 226
  - CIM Browser 221
  - database configuration 212
  - database full 211
  - database initialization error 212
  - DBCS languages, troubleshooting 227
  - discovery 212, 213
  - dynamic groups criteria 216
  - encryption 213, 218
  - event action plans 214, 216
  - event actions 214
  - event ID 2003 221
  - event log error after restarting 221
  - event log full 220
  - FRU information 222
  - IBM Director Agent
    - installing 209, 210
    - modifying 209
    - starting 209, 219
    - timeouts 222
    - uninstalling 211
  - IBM Director Agent Web Server 211
  - IBM Director Console
    - BladeCenter object not displayed 215
    - deleted physical platform object displayed 215
    - discovered systems not displayed 213, 218
    - logon failure 219
    - managed system access request denied 217, 219
    - managed system duplicated 217
    - managed system not displayed 217
    - managed system with question mark 216
    - modifying 209
    - starting 218
    - windows 215
  - IBM Director Server
    - installing 209
- troubleshooting (*continued*)
  - IBM Director Server (*continued*)
    - starting 209, 214
    - uninstalling 211
  - imaging IBM Director Agent 217
  - installation 209
  - insufficient disk space 221
  - Internet Information Services 221
  - Inventory task 220, 222
  - Japanese-language systems 225
  - JRE exceptions 216
  - Korean-language systems 225
  - logical disk drive 221
  - managed systems
    - behind firewall 223
    - encryption 213, 218
    - invalid data values 220
    - resource-monitor information 220
    - running Windows 220
  - management console 215
  - Management Processor Assistant 210, 222, 227
  - management server 211
  - Mass Configuration task 223
  - MIB file attribute values 223, 224
  - Microsoft Internet Explorer 226
  - Microsoft Jet 211
  - Network Configuration task 223
  - network share 224
  - network timeout value, modifying 217
  - PCI adapter 221
  - redirector share 224
  - Remote Access Connection Manager service 220
  - Remote Control task 223
  - Remote Login alerts 211
  - Remote Supervisor Adapter II 222
  - Resource Monitors task 223
  - resource-monitor information 220
  - RPM packages 220, 222
  - RXE-100 discovery 213
  - ServeRAID inventory missing 222
  - Simple Event Filter Builder window 210
  - SNMP devices 213, 223, 224
  - SNMP traps 224
  - Software Distribution task
    - file-distribution server 225
    - managed system behind firewall 224
    - package creation 224
    - software package in SPB format 225
  - Telnet 212
  - time zone error 219
  - timeout associated with large event action plans 214
  - uninstalling
    - Apache error 211
    - error message 1306 211
  - upgrading
    - error message 1306 210
    - error message 1921 210
  - voltage regulator module (VRM) information 221
  - Web-based Access
    - Apache Web Server 226

- troubleshooting (*continued*)
  - Web-based Access (*continued*)
    - event bindings 226
    - Java security warning 226
    - JVM 226
    - Netscape Navigator 226, 227
    - starting 226
    - Win32\_DiskDrive.Size 221
    - won symbols 225
    - yen symbols 225
  - TWGagent.uid file 217
  - TWGConsole.prop file 103, 219
  - TWGIPC service 210, 211
  - twgmach.id file 217
  - TWGserver service 212
  - TWGServer.err file 212
  - TWGServer.prop file 103, 214, 219
  - TWGshare 107
  - twgstat command 215, 218

## U

- UM Services tree, troubleshooting 210
- UMSHTTPD service 210
- unattended installations
  - IBM Director Agent 77, 182, 188
  - IBM Director Console 61, 166
- unattended parameter 62, 78, 83
- unicast discovery 94
- uninstalling IBM Director
  - AIX 204
  - configuration data, retaining 204
  - i5/OS 205
  - Linux 205
  - NetWare 206
  - troubleshooting
    - Apache error 211
    - error message 1306 211
    - locked files 211
  - Windows 206
- updating
  - BIOS code 21, 22
  - device drivers 21, 22
  - firmware 21, 22
- upgrading
  - IBM Director Agent
    - Linux 172
    - NetWare 174
    - Windows 175, 183
  - IBM Director Console
    - Linux 161
    - Windows 161
  - IBM Director Server
    - Linux 150
    - Windows 152
  - Software Distribution task, using 190
  - troubleshooting
    - error message 1306 210, 227
    - error message 1921 210
    - Simple Event Filter Builder window 210
  - upgrading from earlier versions 11

- upward integration 3
- user accounts
  - DirAdmin and DirSuper 33
  - management server running Linux 33
  - management server running Windows 33
  - service account 33
- user administration 97
  - default profile, creating 97
  - DirAdmin group 97
  - DirSuper group 97
  - editing user privileges 99, 100
  - Event Action Plan wizard, restricting access to 99, 102
  - group access, restricting 101
  - task access, restricting 102
- User Administration window 98
- User Defaults Editor 97
- user1.txt 105

## V

- vcredist.exe 71
- Virtual Machine Manager 10
- Virtualization Engine
  - documentation 41
  - IBM Director Multiplatform 3
- voltage regulator module (VRM) information, troubleshooting 221

## W

- Wake on LAN
  - enabling on AIX 66
  - enabling on Linux 198
  - enabling on Windows
    - IBM Director 181, 187
    - IBM Director Agent, installing 76, 82
    - IBM Director Server, installing 51
    - Server, upgrading 159
- WAN link 21
- Web browsers 20
- Web sites
  - IBM Director resources xv
  - IBM eServer Information Center xvi
  - IBM iSeries Information Center 214
  - IBM Redbooks xv
  - IBM ServerProven xvi
  - IBM Support xvi
  - IBM Systems Management Software xvi
  - IBM xSeries Systems Management xvi
  - Net-SNMP 198
  - Oracle Technology Network 31
- Web-based Access
  - configuration files, modifying 226
  - custom access policy, configuring 105
  - event bindings, troubleshooting 226
  - help files 7
  - managed system, installing on 72
  - management server, installing on 46
  - Microsoft Internet Explorer, troubleshooting 226
  - security 35

- Web-based Access *(continued)*
  - troubleshooting 226
    - Java security warning 226
    - JVM 226
    - Netscape Navigator 226, 227
    - starting 226
    - uninstalling 211
  - Web browsers, supported 20
- WIN server names, troubleshooting 223
- windows
  - IBM Director Console
    - Add BladeCenter Chassis 115
    - Director Update Assistant 191
    - IBM Director Login 87
  - Management Module Network Interfaces 116
  - Program Maintenance 204
- windows (IBM Director)
  - Add Physical Platforms 213
  - Capacity Manager installation (NetWare)
    - Choose Destination Location 136
    - Start Copying Files 137
  - Discovery Preferences 213
  - Distribution Preferences 225
  - File Distribution Servers Manager 224
  - IBM Director Agent installation (NetWare)
    - Choose destination location 69
    - InstallShield Wizard complete 70
    - Select Components 69, 175
  - IBM Director Agent installation (Windows)
    - Feature and destination directory selection 72, 176
    - Network driver configuration 76, 181
    - Security settings 73, 178
    - Software Distribution settings 74, 179, 186
    - Web-based Access information 75, 180
- IBM Director Console
  - Add Management Processors 96
  - Add Share Name 108, 111
  - Director Update Assistant 139, 191
  - Discovery Preferences 95, 213
  - IBM Update Package/Root Directory 140, 191
  - Managed System Distribution Preferences 110
  - New Scheduled Job 143, 194
  - Server Preferences 108
  - Software Distribution Manager (Premium Edition) 139, 190
  - Software Distribution Manager (Standard Edition) 138, 190
  - Software Distribution Preferences 109
  - User Administration 98
  - User Defaults Editor 98
- IBM Director Console installation
  - Feature and destination directory selection 59, 164
  - Server Plus Pack 59, 164
- IBM Director Server installation
  - DB2 Universal Database configuration 53
  - Encryption settings 49, 157
  - Feature and installation directory selection 45, 153
  - IBM Director database configuration 52
- windows (IBM Director) *(continued)*
  - IBM Director Server installation *(continued)*
    - Microsoft SQL database configuration 54
    - Network driver configuration 51, 159
    - Oracle database configuration 55
    - Server Plus Pack 45, 153
    - service account information 48, 156
    - Software-distribution settings 50, 157
    - Web-based Access information 50, 158
  - Server Preferences 220, 222
- Windows 2000, troubleshooting 220
- Windows installation
  - encryption, enabling 49, 74
  - IBM Director Agent 71, 78
  - IBM Director Console 58
  - IBM Director Server 44
  - invalid data values 220
  - modifying
    - adding a feature 203
    - installing the IBM Director database 203
    - overview 203
    - removing a feature 203
  - network adapter attribute names, troubleshooting 223
  - Network Configuration task, troubleshooting 223
  - Rack Manager installation, completing 132
  - Server Plus Pack extensions 137
  - troubleshooting
    - event ID 2003 221
    - event log error 221
    - event log full 220
    - Win32\_DiskDrive.Size 221
  - uninstalling 206
- Windows Management Instrumentation (WMI) CORE 1.5 71
- Windows Management Instrumentation (WMI) problem 221
- Windows NT 4.0 installations, prerequisites 71
- Windows Server 2003, troubleshooting 209, 210, 214, 219, 221, 223
- Wired for Management (WfM) specifications 13
- wizards
  - BladeCenter Deployment 117
  - Event Action Plan 88
  - InstallShield
    - IBM Director Agent 71
    - IBM Director Console 58
    - IBM Director Server 44
- wmint4.exe 71
- won symbols, troubleshooting 225
- workers.properties file 226

## X

- xSeries 225, machine type 8647 server 39
- xSeries 360 server 25
- xSeries 440 server 25

## Y

- yen symbols, troubleshooting 225





Part Number: 90P2917

Printed in USA

(1P) P/N: 90P2917

