IBM Director 4.0 for BladeCenter products

Installation and Configuration Guide

SC01-R051-30

Note: Before using this information and the product it supports, read the general information in Appendix C, “Notices” on page 87.

First Edition (November 2002)

Contents

Figures

Tables

Preface

This book provides instructions for installing and configuring IBM® Director 4.0 for BladeCenter™ products.

How this book is organized

Chapter 1, “Introducing IBM Director 4.0 for BladeCenter products” on page 1 contains an overview of IBM Director.

Chapter 2, “Requirements for installing IBM Director” on page 5 contains basic information about IBM Director 4.0 for BladeCenter products. This includes system and network requirements, supported operating systems and database applications, and information about the IBM Director service account.

Chapter 3, “Planning your IBM Director installation” on page 9 provides information about setting up your BladeCenter deployment infrastructure. This chapter also includes information about using Microsoft® SQL Server, Oracle Server, and IBM DB2® Universal Database applications in conjunction with IBM Director.

Chapter 4, “Installing IBM Director Server and IBM Director Console” on page 15 contains instructions for installing IBM Director Server and IBM Director Console.

Chapter 5, “Configuring the IBM BladeCenter chassis” on page 27 contains information about starting IBM Director Console, discovering the BladeCenter chassis, and running the BladeCenter Deployment wizard.

Chapter 6, “Installing IBM Director Agent” on page 43 contains instructions for installing IBM Director Agent.

Chapter 7, “Configuring IBM Director” on page 49 contains information about running the Event Action Plan wizard, setting discovery preferences, and authorizing IBM Director users.

Chapter 8, “Modifying and uninstalling IBM Director” on page 65 contains information about modifying and uninstalling IBM Director.

Chapter 9, “IBM Director Agent — IBM Director Server security” on page 69 contains information about IBM Director security.

Chapter 10, “Solving IBM Director problems” on page 75 lists solutions to problems you might encounter with IBM Director.

Appendix A, “Terminology summary and abbreviation list” on page 81 contains a summary of IBM Director terminology and a list of abbreviations used in IBM Director publications.

Appendix B, “Getting help and technical assistance” on page 85 contains information about accessing IBM Support Web sites for help and technical assistance.

Appendix C, “Notices” on page 87 contains product notices and trademarks.

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 publications

The following publications are available in Portable Document Format (PDF) on the *IBM Director* CD in the /docs directory:

- *IBM Director 4.0 for BladeCenter products Installation and Configuration Guide* (dir40_install.pdf)
- *IBM Director 4.0 for BladeCenter products Systems Management Guide* (dir40_sysmgt.pdf)

In addition, the following IBM Redbooks™ publications might be of interest:

- *IBM @server BladeCenter Systems Management* (REDP3582)
- *The Cutting Edge: IBM @server BladeCenter* (REDP3581)
- *Deploying Microsoft Exchange on IBM @server BladeCenter* (REDP3585)
- *Deploying Lotus Domino on IBM @server BladeCenter* (REDP3584)
- *IBM @server BladeCenter Type 8677 Planning and Installation Guide* (GA27-4327-00)
- *Managing IBM TotalStorage NAS with IBM Director* (SG24-6830-00)
- *IBM Director Security* (REDPO417)
- *Implementing IBM Director Management Solutions* (SG 24-6188-00)
- *Integrating IBM Director with Enterprise Management Solutions* (SG24-5388-01)
- *Implementing Asset ID* (SG 24-6165-00)

You can download these books from the IBM Web site at http://www.ibm.com/redbooks/.

Note: Some of the Redbooks publications contain outdated information. 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 Online Assistant and e-Mail

http://www.ibm.com/pc/qtechinfo/MIGR-4Z7HJX.html

This Web page offers a quick resource to help solve your technical questions. Follow the instructions on this page to find additional solutions for your systems-management tools.

If you do not find an acceptable solution, or if you just want to bypass looking for your own solution, you can submit an electronic question. From

any page within the IBM Online Assistant, click **None of the above** to submit an electronic inquiry. Response times vary between 24 and 48 hours.

IBM Universal Manageability Discussion Forum
http://www7.pc.ibm.com/~ums/

IBM forums put you in contact with other IBM users. The forums are monitored by IBM technicians.

IBM Systems Management Software: Download/Electronic Support page
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.

IBM xSeries Systems Management page
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. Click **IBM Director 4.1** for the latest information and publications about the next release of IBM Director.

Systems Management - Quick Reference Guide
http://www.ibm.com/pc/qtechinfo/MIGR-4WEP53.html?

This Web page includes links to software downloads, eFixes, Microsoft® Service Packs, and publications for supported releases of IBM Director.

IBM Universal Manageability page
http://www.ibm.com/pc/us/pc/um/index.html

This Web page links to an IBM portfolio of advanced management tools that help lower costs and increase availability throughout the life cycle of a product.

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**.

If you are preparing to install IBM Director and you need to download updates for your server, click **Servers** on the IBM Support Web site. The IBM xSeries™, Netfinity®, and PC Server support Web page opens. On the left, click **Downloadable files**. The **Downloadable files by category** drop-down list is displayed. Click the category of downloadable files that you need. If you want to use Update*Xpress*™ to update your server, on the right click **UpdateXpress CD** for the latest release of Update*Xpress*.

Chapter 1. Introducing IBM Director 4.0 for BladeCenter products

IBM Director is a comprehensive systems-management solution. A powerful suite of tools and utilities, IBM Director automates many of the processes required to manage systems proactively, including preventive maintenance, diagnostic monitoring, troubleshooting, and more. It offers a graphical user interface that provides system administrators easy access to both local and remote systems. IBM Director can be used in environments with multiple operating systems (heterogeneous environments).

IBM Director 4.0 for BladeCenter products is a version of IBM Director released for use with IBM @server BladeCenter and @server BladeCenter HS20 *only*.

Important

IBM Director 4.0 for BladeCenter products is supported *only* for use managing BladeCenter chassis and blade servers.

IBM Director 3.x and IBM Director 4.0 for BladeCenter products cannot be installed on the same system. For example, you cannot install IBM Director Server 3.x and IBM Director Server 4.0 on the same server, nor can you run IBM Director Console 3.x and IBM Director Console 4.0 on the same system.

While both versions of IBM Director can coexist in an environment, you must take care to ensure that IBM Director Server 3.x manages *only* systems running IBM Director Agent 3.x and that IBM Director Server 4.0 manages *only* systems running IBM Director Agent 4.0. If you have an existing IBM Director 3.x environment, consider taking the following actions:

- Installing IBM Director 4.0 on a separate subnet.
- Using unicast discovery only, to ensure that IBM Director Server 4.0 discovers *only* blade servers running IBM Director Agent 4.0.
- Ensure that all managed systems running IBM Director Agent 3.x are secured.

You cannot upgrade to IBM Director 4.0 for BladeCenter products from any previous version of IBM Director. Nor will you be able to upgrade from IBM Director 4.0 for BladeCenter products to IBM Director 4.1. However, you can uninstall IBM Director 4.0 for BladeCenter products and install IBM Director 4.1.

IBM Director 4.1 will include support for migrating such management server data as event action plans and thresholds.

IBM Director components

The hardware in an IBM Director environment can be divided into the following groups:

- One or more servers on which IBM Director Server is installed. Such servers are called *management servers*.
- Systems that are managed by IBM Director. Such systems are called *managed systems*.
- Network drivers, printers, or computers that have SNMP agents installed or embedded. Such devices are called *SNMP devices*.

The IBM Director software has three components: IBM Director Server, IBM Director Agent, and IBM Director Console. Each group of hardware in your IBM Director environment requires a different combination of these components.

All three components (IBM Director Server, IBM Director Console, and IBM Director Agent) must be installed on the management server. IBM Director Agent must be installed on each managed system. IBM Director Console must be installed on any system (called a *management console*) from which a system administrator will remotely access the management server. IBM Director software does not need to be installed on SNMP devices.

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. You can use the Microsoft Jet 4.0 database engine, which is included in Microsoft Windows® 2000, or you can use another database application.

When you install IBM Director Server, IBM Director Console and IBM Director Agent are installed automatically.

IBM Director Server can be installed on the following operating systems:

- Windows 2000 Server (Service Pack 3 required)
- Windows 2000 Advanced Server (Service Pack 3 required)

IBM Director Server requires a license. Every IBM xSeries server and @server BladeCenter chassis comes with an IBM Director Server license.

IBM Director Agent

IBM Director Agent provides management data to IBM Director Server. Data can be transferred using several network protocols, including TCP/IP, NetBIOS, IPX, and SNA. IBM Director Server can communicate with all systems in your network that have IBM Director Agent installed.

IBM Director Agent can be installed on the following operating systems:

- Windows 2000 Advanced Server (Service Pack 3 required)
- Windows 2000 Server (Service Pack 3 required)
- Red Hat Linux®, version 7.3
- SuSE Linux, version 8.0

IBM Director Console

IBM Director Console is the graphical user interface (GUI) for IBM Director Server. Data is transferred between IBM Director Console and IBM Director Server through TCP/IP. Using IBM Director Console, system administrators 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 also must install IBM Director Agent on that system.

IBM Director Console can be installed on the following operating systems:

- Windows 2000 Advanced Server (Service Pack 3 required)
- Windows 2000 Server (Service Pack 3 required)
- Windows 2000 Professional (Service Pack 3 required)
- Windows XP Professional (Service Pack 1 recommended)

IBM Director Agent features

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

System Health Monitoring (Windows only)

System Health Monitoring provides active monitoring of critical system functions, including disk space availability, drive alerts, temperatures, and power supply voltage. It produces and relays hardware alerts.

Note: You *must* install System Health Monitoring if you want to monitor the managed system hardware and send alerts.

SNMP Access and Trap Forwarding

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

Note: If you want IBM Director Server to poll SNMP devices and receive their alerts, verify that the Windows SNMP Service and Windows SNMP Trap Service are running on the management server.

Chapter 2. Requirements for installing IBM Director

This chapter contains information about system and network requirements, licenses, and supported database applications. It also contains information about the IBM Director service account.

System requirements

This section contains information about hardware requirements and supported operating systems.

Hardware configuration

The systems on which you install IBM Director Server or IBM Director Agent 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. Minimum hardware requirements for IBM Director

	IBM Director Server	**IBM Director Agent**	**IBM Director Console**
Microprocessor speed	Pentium 300+ MHz	Pentium class processor	Pentium 300+ MHz
Memory (RAM)	256 MB (512 MB recommended)	128 MB	128 MB
Disk space	300 MB	100 MB	160 MB

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 management console.

BIOS, device drivers, and firmware

SMBIOS 2.1 or later is required for all systems in an IBM Director environment.

Supported operating systems

The IBM Director software components have different levels of operating-system support.

IBM Director Server

IBM Director Server is supported on the following operating systems:

- Windows 2000 Advanced Server (Service Pack 3 required)
- Windows 2000 Server (Service Pack 3 required)

IBM Director Agent

IBM Director Agent is supported on the following operating systems:

- Windows 2000 Advanced Server (Service Pack 3 required)
- Windows 2000 Server (Service Pack 3 required)
- Red Hat Linux, version 7.3
- SuSE Linux, version 8.0

IBM Director Console

IBM Director Console is supported on the following operating systems:

- Windows XP Professional (Service Pack 1 recommended)
- Windows 2000 Professional (Service Pack 3 required)
- Windows 2000 Server (Service Pack 3 required)
- Windows 2000 Advanced Server (Service Pack 3 required)

Network requirements

This section discusses supported network protocols, as well as ports used in an IBM Director environment.

Network protocols

IBM Director Server communicates with the IBM Director Console only through TCP/IP. You can use TCP/IP, NetBIOS, SNA, or IPX to communicate between IBM Director Server and IBM Director Agent. IBM Director Server communicates with SNMP devices only through TCP/IP.

Note: TCP/IP is the only network protocol that you can use to communicate with managed systems running Linux.

The following table lists the supported versions of network protocols.

Table 2. Network protocols

Protocol	Supported version
TCP/IP	All WinSock-compatible versions of TCP/IP supported by Windows 2000, NetWare 6.0, Linux, and UNIX
NetBIOS	Native NetBIOS versions supported by Windows 2000
IPX	IPX versions supported by NetWare 6.0 and Windows 2000
SNA	Microsoft SNA 4.0 with Service Pack 1

Ports

The following table lists the ports used by IBM Director.

Table 3. Ports used by IBM Director

	Connection	IP port	IPX ports
IBM Director	IBM Director Server → BladeCenter chassis	427 UDP and TCP	
	IBM Director Server → IBM Director Agent	14247 UDP and TCP	4490 (hex) read 4491 (hex) write
	IBM Director Agent → IBM Director Server		
	IBM Director Server → IBM Director Console	Random*	
	IBM Director Console → IBM Director Server	2033 TCP*	
	SNMP access	161 UDP	
	SNMP traps	162 UDP	
Service processors	Telnet to service processors	23 TCP	
	IBM Director → service processor	6090 TCP	
	SNMP agent	161 UDP	
	SNMP traps	162 UDP	
	LAN alerts	13991 UDP	

* IBM Director Console opens a port in the 1024 - 65535 range. Then it connects through TCP to IBM Director Server using port 2033. When IBM Director Server responds to IBM Director Console, it communicates to the random port in the 1024 - 65535 range that IBM Director Console opened.

Licensing

IBM Director 4.0 includes the following licenses:

- One license for the installation of IBM Director Server (which automatically includes IBM Director Agent and IBM Director Console)
- Unlimited licenses to install IBM Director Console

All IBM @server BladeCenter HS20 servers come with a license for IBM Director Agent.

Database

IBM Director requires a SQL database to store the system inventory data. You can use the following database applications in conjunction with IBM Director:

- Microsoft Jet 4.0 database engine, Service Pack 6, and Microsoft Data Access Control (MDAC) 2.7
- Microsoft SQL Server 7.00, Service Pack 3, and MDAC 2.7
- Microsoft SQL Server 2000, Service Pack 2, and MDAC 2.7
- Microsoft SQL Server 2000 Desktop Engine, Service Pack 2, and MDAC 2.7
- Microsoft Data Engine 1.0, Service Pack 3, and MDAC 2.7

- Oracle Server versions 8.1.7 or 9.0.x
- IBM DB2 Universal Database 7.2, Fix Pack 6
- IBM DB2 Universal Database 6.1, Fix Pack 10

The Microsoft Jet 4.0 database engine is built into Windows 2000. However, the Jet database has a 2.14 GB limit. Typically, an environment with more than 300 to 500 managed systems should *not* use the Microsoft Jet 4.0 database.

If you plan to use a database application other than Microsoft Jet, you should install and configure the database application *before* installing IBM Director Server.

Security and accounts

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

Note: It is a best practice to use the IBM Director service account *only* for IBM Director system administration.

Chapter 3. Planning your IBM Director installation

This chapter provides information about setting up the BladeCenter deployment infrastructure. It also includes information about selecting and configuring a database application to use with IBM Director.

Setting up the BladeCenter deployment infrastructure

You must use a non-blade server as the management server. This will ensure that you can run the BladeCenter Deployment wizard and use the BladeCenter tasks. Only one management server can communicate with the BladeCenter management module at any one time.

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

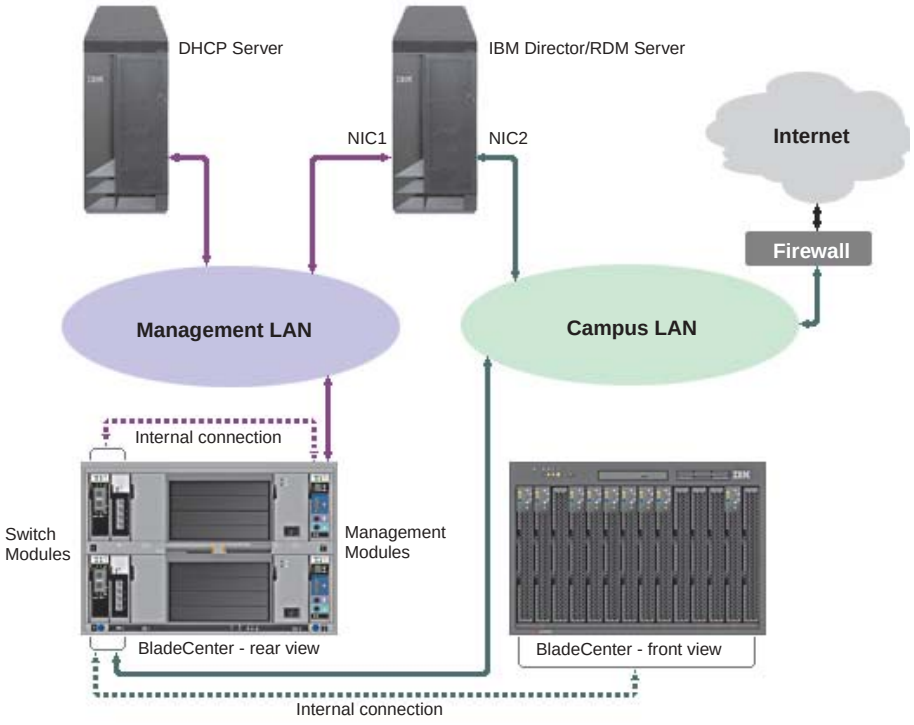

Figure 1. Example of a BladeCenter deployment network

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

Consider using a DHCP server to assign a temporary 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 a non-routable 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 run the BladeCenter Deployment wizard and 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 3.1.01 and Patch 2 on the management LAN also.

Note: RDM 3.1.01 and Patch 2 are available on the *IBM @server BladeCenter Resource* CD.

If you plan to use SQL Server or DB2, consider installing the database server on the management LAN also. If the management server is in a different domain, there must be a trust relationship between the two domains.

Database management

IBM Director supports the following database applications:

- Microsoft Jet 4.0 database engine, Service Pack 6, and Microsoft Data Access Control (MDAC) 2.7
- Microsoft SQL Server 7.00, Service Pack 3, and MDAC 2.7
- Microsoft SQL Server 2000, Service Pack 2, and MDAC 2.7
- Microsoft SQL Server 2000 Desktop Engine, Service Pack 2, and MDAC 2.7
- Microsoft Data Engine 1.0, Service Pack 3, and MDAC 2.7
- Oracle Server versions 8.1.7 or 9.0.x
- IBM DB2 Universal Database 7.2, Fix Pack 6
- IBM DB2 Universal Database 6.1, Fix Pack 10

If you plan to use a database application other than Microsoft Jet, your database administrator must prepare the database application before you install IBM Director Server.

Determine an appropriate size for the database. If you intend to manage 300 to 500 systems, depending on the amount of inventory that is being generated by each managed system, an initial size of 100 MB is sufficient. You might need a larger database if you manage additional systems or have extensive inventory data.

The *database server* is the server on which the database application is installed.

Microsoft Jet 4.0

IBM Director comes with the Microsoft Jet 4.0 database engine. The Microsoft Jet database engine creates a single database file that is installed on the management server. The database has a maximum size of 2.14 GB. If you plan to manage more than 300 to 500 systems, use another database application.

IBM DB2 Universal Database

To use DB2, you must complete the following tasks before installing IBM Director Server:

- Install the DB2 Administration Client on the management server
- Configure DB2 to use the Java® Database Configuration (JDBC) 2.0 driver
- Set up a trusted connection, if used
- Give the IBM Director service account access to DB2
- Create the DB2 database or give the IBM Director service account Create Database permission

Note: If you have a remote connection to DB2, you must have a node entry for the database server.

Installing the DB2 Administration Client

Complete the following steps to install the DB2 Administration Client:

1. Install the DB2 Administration Client on the management server. Be sure to install the following components.

Version 6.1	Version 7.2
• Communications protocols • ODBC support • Java enablement • System bind files	• Communications protocols • Applications Development Interface • Base DB2 client support • System bind files

2. Verify that the CLASSPATH points to the db2java.zip directory that contains the DB2 JDBC driver.

Configuring DB2 to use the JDBC 2.0 driver

Note: IBM Director Server requires the JDBC 2.0 driver. For more information about the JDBC 2.0 driver, see the release notes for DB2, version 7.2. You can download the release notes from the IBM Web site at www.ibm.com (type `JDBC 2.0 driver` in the **Search field**).

Complete the following steps to configure DB2 to use the JDBC 2.0 driver:

1. From a command prompt, type the following command and press Enter:

   ```
   cd sqllib\java12
   ```

   where *sqllib* is the directory where DB2 is installed.
2. Ensure that the DB2 JDBC Applet Server and the DB2 JDBC Applet Server-Control Center services are stopped.

3. From the command prompt, type the following command and press Enter:

   ```
   usejdbc2
   ```

   Issuing this command creates a sqllib\java11 directory, backs up the JDBC 1.22 driver files into the sqllib\java11 directory, and makes the JDBC 1.22 driver the default.
4. Verify that all of the files are copied to the sqllib\java and sqllib\bin directories.

   If the message `Access is denied. The process cannot access the file because it is being used by another process` is displayed, one or more services might be running. Complete the following steps:

   a. From the Windows Services window, stop all DB2 Services.
   b. From a command prompt, type the following command and press Enter:

      ```
      usejdbc2
      ```

   c. If errors continue, issue the db2stop force command and issue the usejdbc2 command again.

Setting up trusted connections

If you use trusted connections, set the database server security to support trusted connections. See the *DB2 Administration Guide* for information about trusted IBM DB2 client scenarios.

Configuring DB2 Server login access for IBM Director

The IBM Director service account database must be authorized to log on to DB2 Server. For additional information about DB2 security, see the *DB2 Administration Guide*.

Creating the DB2 Server database

You can create the DB2 database either before or during the IBM Director Server installation. To create the DB2 Server database during the IBM Director Server installation, the database administrator must give the IBM Director service account Create Database authority. If you do not want this level of authority, the database administrator must create the database manually (that is, before the IBM Director Server installation).

Creating the database before installing IBM Director Server: The database administrator must complete the following steps:

1. Create the database.
2. Do one of the following:
   - Transfer ownership of the database to the IBM Director service account
   - Give the IBM Director service account user-level access to the database, as well as Create Table permission
3. Provide the following information to the system administrator who will install IBM Director Server:
   - The name of the server where DB2 Server is located
   - The name of the database

Creating the database while installing IBM Director Server: The database administrator must complete the following steps:

1. Give the IBM Director service account Create Database permission on the DB2 Server database.
2. Provide the following information to the system administrator who will install IBM Director Server:
   - The name of the server where DB2 Server is located
   - The name of the database

Microsoft SQL Server

To use Microsoft SQL Server, you must complete the following tasks before installing IBM Director Server:

- Set up a trusted connection (if used)
- Authorize the IBM Director service account to access Microsoft SQL Server
- Create the Microsoft SQL Server database or give the IBM Director service account Create Database permission in the master database. For more information, see “Creating the database before installing IBM Director Server”.

Setting up trusted connections

If you use trusted connections, set the database server security to support trusted connections. If you configure the database server for mixed security, you also must authorize the IBM Director service account to access Microsoft SQL Server.

Authorizing the service account to access Microsoft SQL Server

The IBM Director service account must be authorized to log on to Microsoft SQL Server. For more information on Microsoft SQL Server, see the documentation that comes with this product.

Creating the Microsoft SQL Server database

You can create the Microsoft SQL Server database either before or during the IBM Director Server installation. To create the Microsoft SQL Server database during the IBM Director Server installation, the database administrator must give the IBM Director service account Create Database permission in the master database. If you do not want this level of authority, the database administrator must create the database manually (that is, before the IBM Director Server installation).

Creating the database before installing IBM Director Server: The database administrator must complete the following steps:

1. Create the database.
2. Do one of the following:
   - Transfer ownership of the database to the IBM Director service account
   - Give the IBM Director service account user-level access to the database file and Create Table permission
3. Provide the following information to the system administrator who will install IBM Director Server:
   - The name of the server where the Microsoft SQL Server database is located
   - The name of the database

Creating the database while installing IBM Director Server: The database administrator must complete the following steps:

1. Give the IBM Director service account Create Database permission in the master database.

   Note: When the database is created during the IBM Director installation, the size of the database defaults to the larger of the following:
   - The size of the model database
   - The default database size specified in the Microsoft SQL Server configuration options

2. Provide the system administrator who will install IBM Director Server with the following information:
   - The name of the server where Microsoft SQL Server is located
   - The name of the database

Oracle Server

To use Oracle Server, you must complete the following tasks before installing IBM Director Server:

- Create the Oracle Server database
- Configure and start the Oracle TCP/IP listener

Creating the Oracle Server database

The database administrator must create the Oracle Server database before IBM Director Server is installed. During the installation of IBM Director Server, the following information is required:

- Oracle TCP/IP listener port
- TCP/IP host name of the Oracle Server (this information is needed when you begin configuring IBM Director 4.0 with this database application)
- Oracle system identifier
- Oracle administrator account ID and password

The Oracle administrator account ID and password are used to create tablespaces, a role (TWG_ROLE), and assign a user ID and password. IBM Director *does not* save the Oracle administrator account ID and password.

Configuring the Oracle TCP/IP listener

IBM Director Server uses the Oracle JDBC client-side driver to connect to Oracle Server. This is a JDBC Type 4 driver. It emulates the Oracle SQL *Net, Net8, and TTC adapters by using its own TCP/IP-based Java socket implementation. The Oracle JDBC client-side driver does not require Oracle client software to be installed. However, it does require that the Oracle Server be configured with a TCP/IP listener.

Configure and start the Oracle TCP/IP listener before installing IBM Director Server.

Chapter 4. Installing IBM Director Server and IBM Director Console

This chapter describes how to install IBM Director Server and IBM Director Console.

Installing IBM Director Server

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 will have the opportunity to install several IBM Director Agent features.

IBM Director Server can be installed on the following operating systems:

- Windows 2000 Server (Service Pack 3 required)
- Windows 2000 Advanced Server (Service Pack 3 required)

Complete the following steps to install IBM Director Server:

1. Log on to the operating system with the IBM Director service account. (For more information, see “Security and accounts” on page 8.)
2. Insert the *IBM Director 4.0* 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 **Install IBM Director Server**. 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 of the license agreement**; then, click **Next**. The “Feature and installation directory selection” window opens.

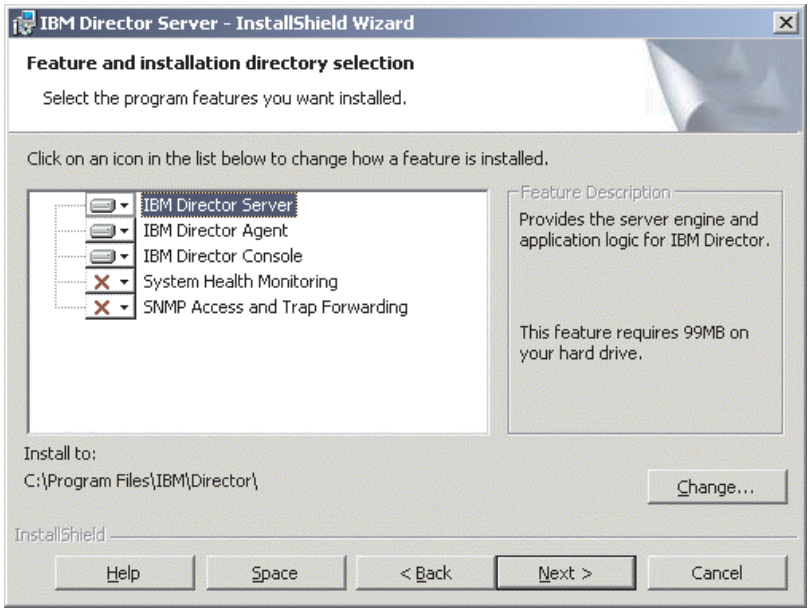

Figure 2. Installing IBM Director Server: "Feature and installation directory selection" window

9. IBM Director Server, IBM Director Agent, and IBM Director Console are selected for installation automatically; a hard disk icon  is displayed to the left of each component.  is displayed to the left of the optional features.

   You can install the following optional features:

   System Health Monitoring
   Monitors the status of hardware components; produces and relays hardware alerts.

   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.

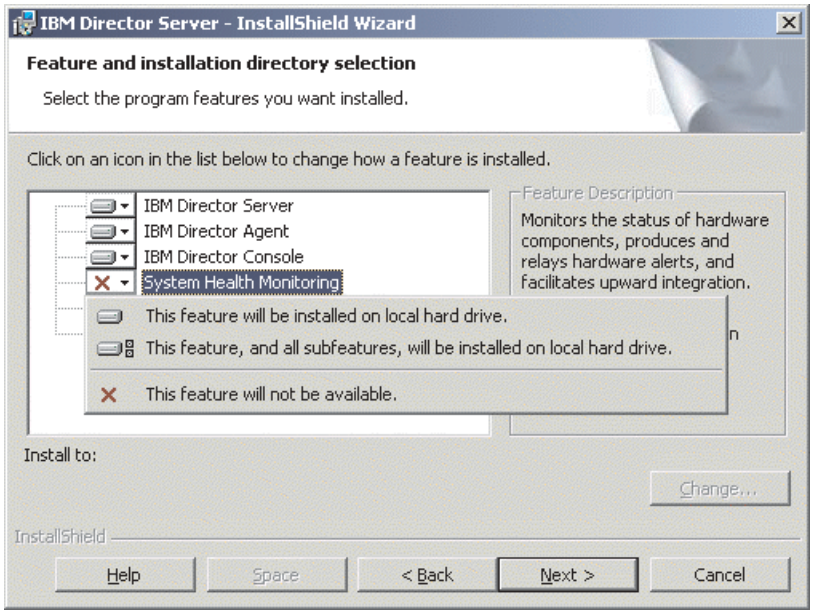

Figure 3. Installing IBM Director Server: "Features and installation directory selection" window

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

10. Click **Next**. The "IBM Director service account information" window opens. (For more information about the IBM Director service account, see "Security and accounts" on page 8.)

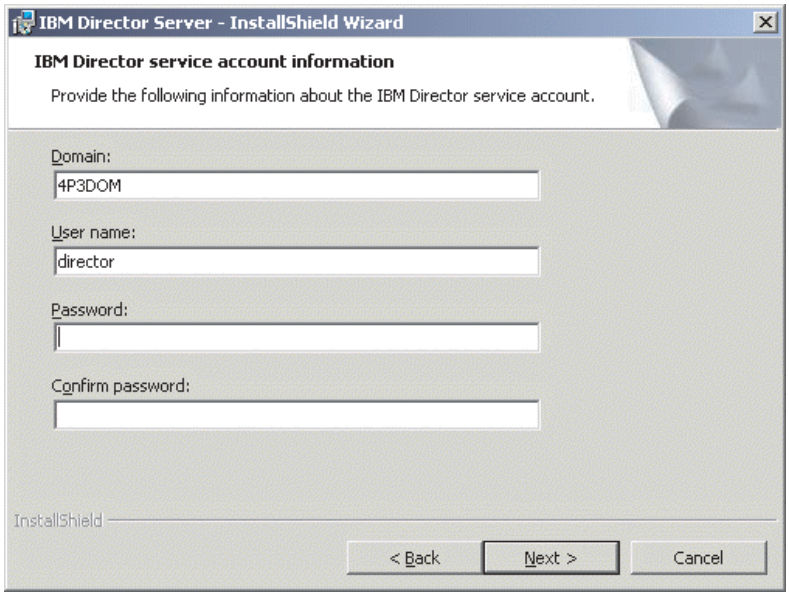

Figure 4. Installing IBM Director Server: "IBM Director service account information" window

11. In the **Domain** field, type the domain of the IBM Director service account.
12. In the **User name** field, type the user ID for the IBM Director service account.
13. In the **Password** and **Confirm password** fields, type the password for the IBM Director service account.

14. Click **Next**. The “Software-distribution settings” window opens.

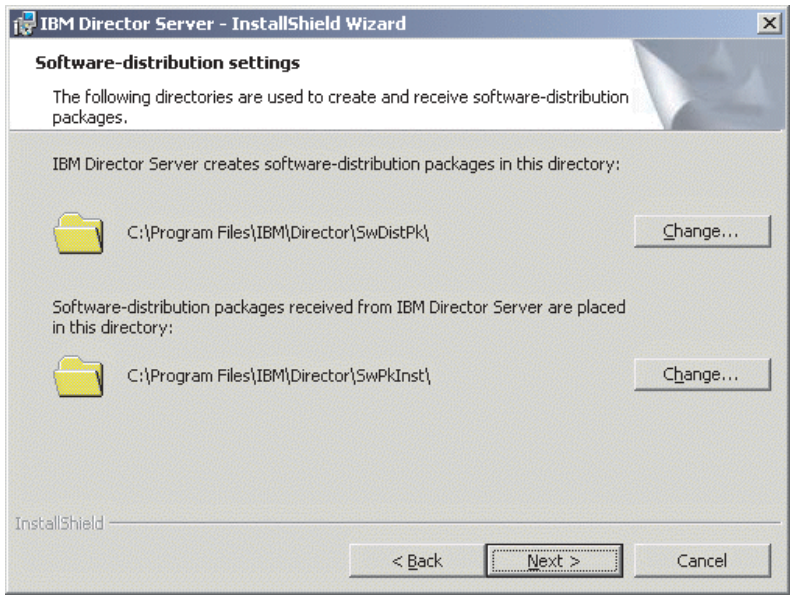

Figure 5. Installing IBM Director Server: “Software-distribution settings” window

15. To select an alternate location for where IBM Director Server creates software-distribution packages, click **Change** and select another directory.

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

16. Click **Next**. The “Network driver configuration” window opens.

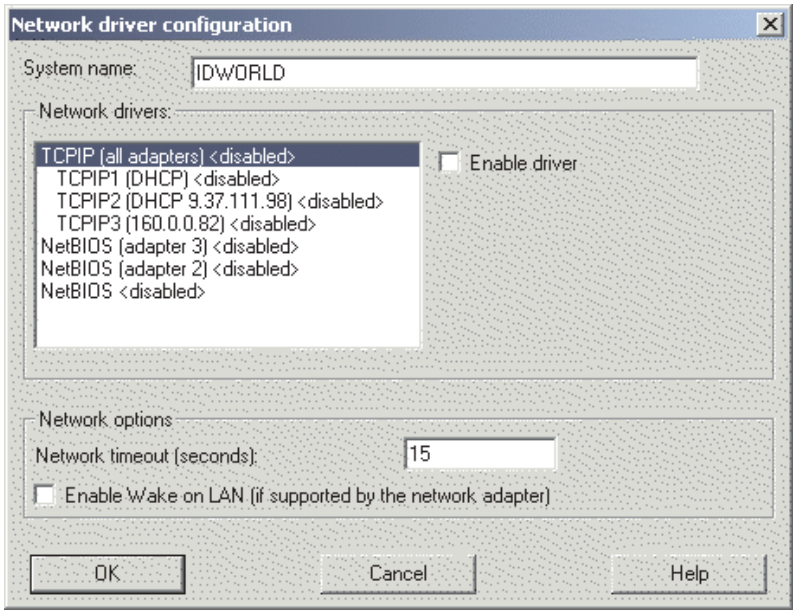

Figure 6. Installing IBM Director Server: “Network driver configuration” window

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 management server.
18. To enable a network driver, select the communication protocol you are using in your network (such as TCP/IP or NetBIOS) and select the **Enable driver** check box.

    In the **Network timeout** field, type the number of seconds that IBM Director Server will wait for a response from IBM Director Agent. By default, this is set to 15 seconds.

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

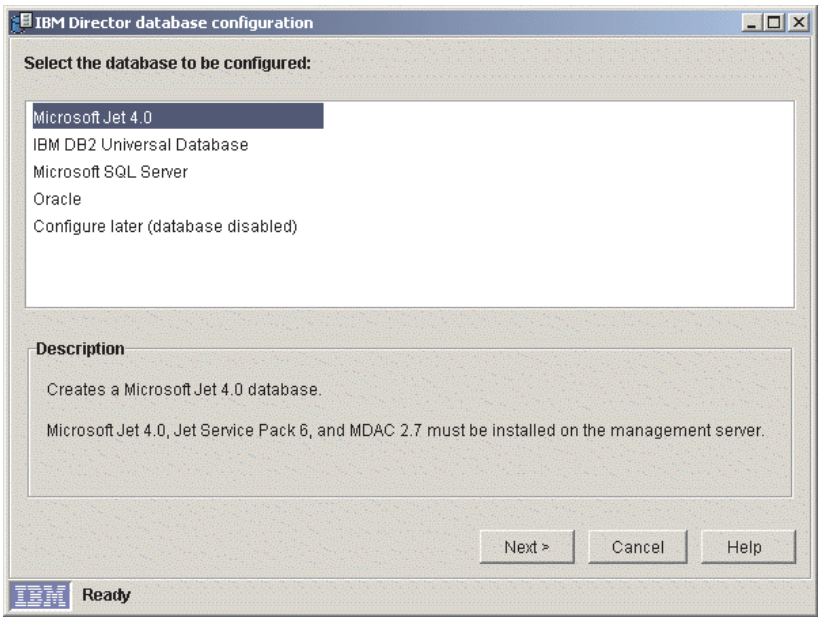

Figure 7. Installing IBM Director Server: “IBM Director database configuration” window

20. Click the database application 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 6, and MDAC 2.7 must be installed on the management server.

    IBM DB2 Universal Database
    Creates a DB2 database. Either DB2 Administration Client or IBM DB2 Universal Database must be installed and configured on the management server.

    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 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.

21. Click **Next**. Do one of the following:

If you selected	Go to
Microsoft Jet 4.0	Step 28 on page 23
IBM DB2 Universal Database	Step 22
Microsoft SQL Server	Step 24 on page 21
Oracle	Step 25 on page 21
Configure later (database disabled)	Step 28 on page 23

22. The “IBM Director DB2 Universal Database configuration” window opens.

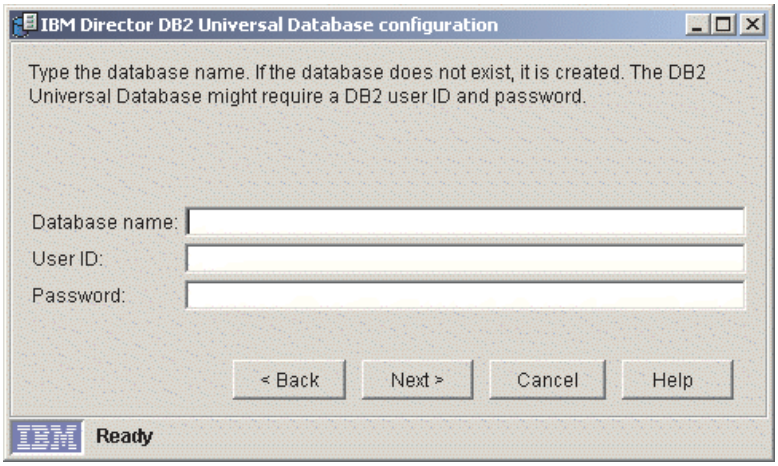

Figure 8. Installing IBM Director Server: “IBM Director DB2 Universal Database configuration” window

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.
c. In the **Password** field, type the password for the DB2 user ID.

23. Click **Next**. The second “IBM Director DB2 Universal Database configuration” window opens.

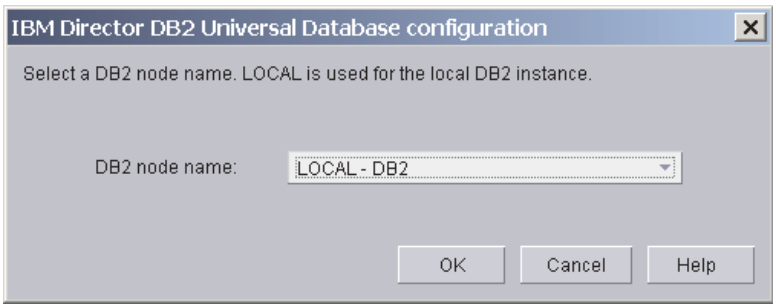

Figure 9. Installing IBM Director Server: "IBM Director DB2 Universal Database configuration" window

In the **DB2 node name** field, select the location of the DB2 database. Then click **OK** and go to step 28 on page 23.

24. The "IBM Director Microsoft SQL Server database configuration" window opens.

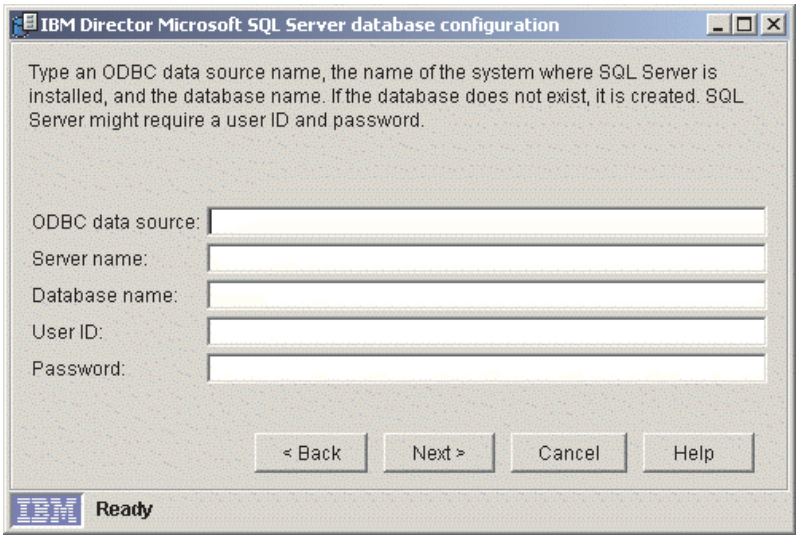

Figure 10. Installing IBM Director Server: "IBM Director Microsoft SQL Server database configuration" window

a. In the **ODBC data source** field, type the ODBC data source name.
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.
e. In the **Password** field, type the password for the SQL Server user ID (if required).

Click **Next**. Go to step 28 on page 23.

25. The "IBM Director Oracle database configuration" window opens.

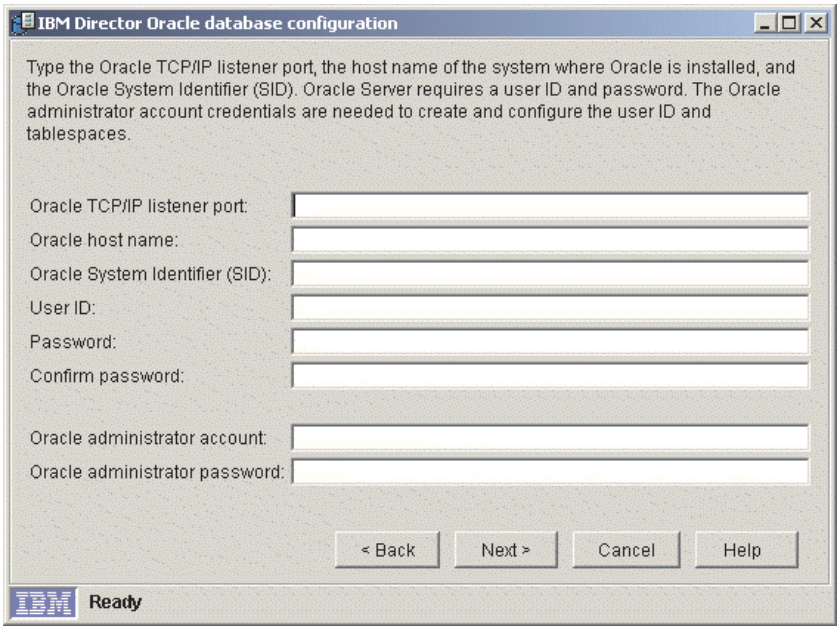

Figure 11. Installing IBM Director Server: "IBM Director Oracle database configuration" window

a. In the **Oracle TCP/IP listener port** field, type the number of the port used by the Oracle TCP/IP listener.

b. In the **Oracle host name** field, type the TCP/IP host name of the Oracle 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 will be assigned to the IBM Director tablespace.

e. In the **Password** and **Confirm password** fields, type the password associated with the user ID you typed in step 25d.

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 associated with the user ID you typed in step 25f.

26. Click **Next**. The second "IBM Director Oracle database configuration" window opens.

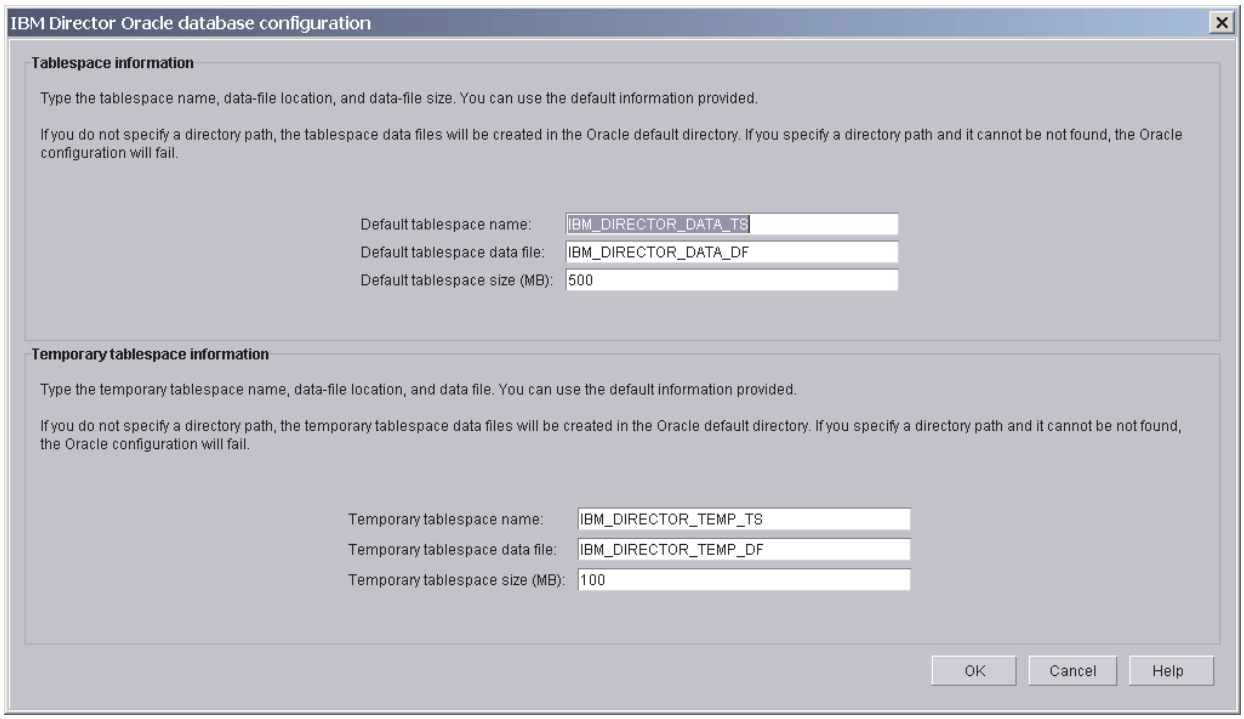

Figure 12. Installing IBM Director Server: "IBM Director Oracle database configuration" window

27. Type information in the following entry fields:

    Tablespace information

    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.

    Temporary tablespace information

    a. In the **Temporary tablespace name** field, type a name for the temporary tablespace.

    b. 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.

    c. In the **Temporary tablespace size (MB)** field, type the size of the temporary tablespace in MB.

    Click **OK**.

28. The status bar displays the progress of the installation. When the installation is complete, the InstallShield Wizard Completed window opens.
29. Click **Finish**. A window opens, asking you if you want to restart the server.
30. Click **Yes** to restart the server.

Installing IBM Director Console

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.

IBM Director Console can be installed on the following operating systems:

- Windows XP Professional (Service Pack 1 recommended)
- Windows 2000 Advanced Server (Service Pack 3 required)
- Windows 2000 Server (Service Pack 3 required)
- Windows 2000 Professional (Service Pack 3 required)

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.

Installing IBM Director Console using the InstallShield wizard

Complete the following steps to install IBM Director Console:

1. Insert the *IBM Director 4.0* 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 **Install IBM Director Console**. The Welcome to the InstallShield Wizard window opens.
6. Click **Next**. The License Agreement window opens.
7. Click **I accept the terms of the license agreement**; then, click **Next**. The “Feature and installation directory selection” window opens.

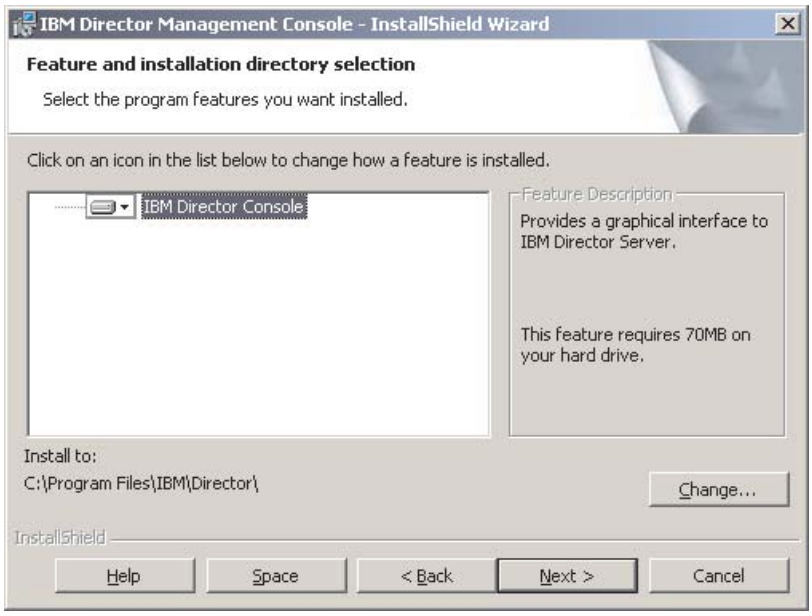

Figure 13. Installing IBM Director Console: "Feature and installation directory selection" window

IBM Director Console is selected for installation automatically.

8. Click **Next**. The Ready to Install the Program window opens.
9. Click **Install**. The Installing IBM Director Management Console window opens.

   The status bar displays the progress of the installation. When the installation is complete, the InstallShield Wizard Completed window opens.
10. Click **Finish**.
11. Remove the 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 posed by the InstallShield wizard. A system administrator 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 4.0* CD into the CD-ROM drive.
2. Copy the dircon.rsp file to a local directory. This file is located in the director\console\windows\i386 directory on the *IBM Director 4.0* 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 ASCII text editor.
5. Modify and save the dircon.rsp file. This file follows the Windows .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 located in the director\console\windows\i386 directory on the *IBM Director 4.0* 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 on page 25.

8. When the installation is complete, remove the CD from the CD-ROM drive.

Chapter 5. Configuring the IBM BladeCenter chassis

After installing IBM Director Server, you can discover the BladeCenter chassis and run the BladeCenter Deployment wizard. After the BladeCenter chassis is configured, you can install the operating systems on the blade servers. You can do this manually or by using RDM.

Starting IBM Director Console

After installing IBM Director Server, complete the following steps to start IBM Director Console:

1. Verify that the IBM Director Server is running. Check to see if the task bar in the lower-right corner of the screen contains a bright green circle.
2. Click **Start → Programs→ IBM Director Console**. The IBM Director Login window opens.

Figure 14. IBM Director Login window

3. In the **IBM Director Server** field, type the name of the management server.
4. In the **User ID** field, type:

   `DirectorUserID`

   where *DirectorUserID* is a valid IBM Director user ID.
5. In the **Password** field, type the password that corresponds to the user name.
6. Click **OK**. IBM Director Console opens.

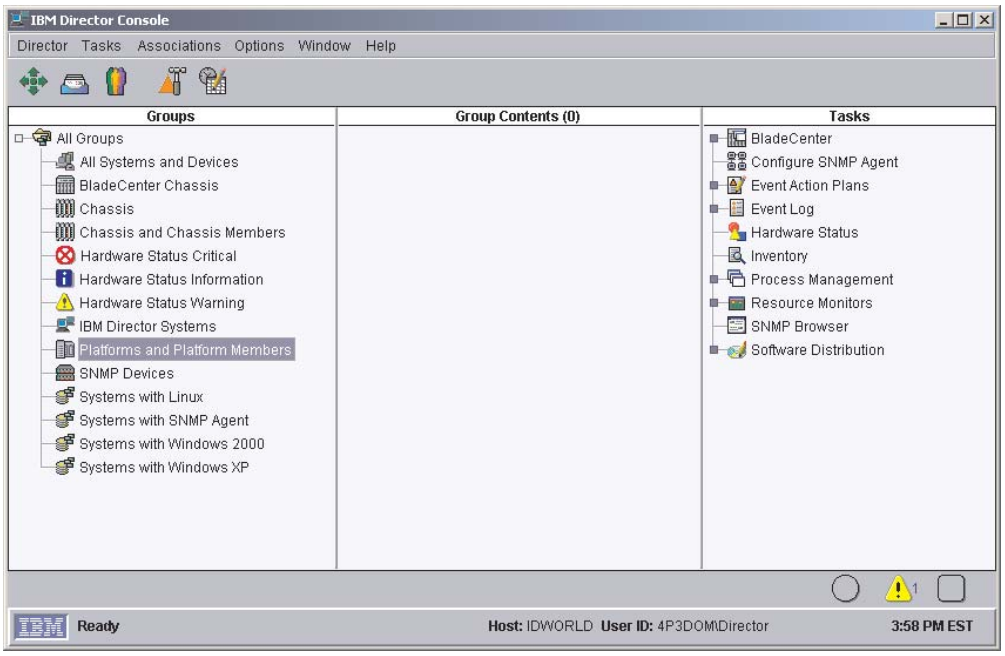

Figure 15. IBM Director Console window

Discovering a BladeCenter chassis

Before you can run the BladeCenter Deployment wizard and configure the BladeCenter chassis, IBM Director must discover the BladeCenter chassis and create a BladeCenter chassis managed object.

IBM Director discovers 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 a non-routable IP address (192.168.70.125) to the external management port.

If the management server and the BladeCenter chassis are on the same subnet, IBM Director can discover the BladeCenter chassis automatically. You either must use a DHCP server to assign a temporary IP address to the BladeCenter chassis or manually assign the management module a static IP address on the same subnet as the management server. Go to “Automatically discovering the BladeCenter chassis” on page 29.

If the management server and the BladeCenter chassis are not on the same subnet, you must manually create the BladeCenter chassis managed object. Go to “Manually creating a BladeCenter chassis managed object” on page 29.

Note: If DHCP is not used, only one BladeCenter chassis can be introduced onto the network at a time. IBM Director 4.0 must discover and configure the chassis before another chassis is added to the LAN. Otherwise, an IP address conflict will ensue.

Automatically discovering the BladeCenter chassis

IBM Director uses the Service Location Protocol (SLP) to discover the BladeCenter management module and create a BladeCenter chassis managed object.

The management server and the BladeCenter chassis must be connected to the network and on the same subnet. You must assign a valid IP address to the external port of the BladeCenter management module. One of the following conditions must be true:

- The network contains a DHCP server which has assigned a temporary IP address to the management module.
- You have manually changed the default, non-routable IP address of the management module to a valid IP address.

Complete the following steps to discover the BladeCenter management module and create a BladeCenter chassis managed object:

1. Start IBM Director Console.
2. Click **Tasks → Discover Systems → BladeCenter Chassis**.
3. The BladeCenter chassis managed object is displayed in IBM Director Console.

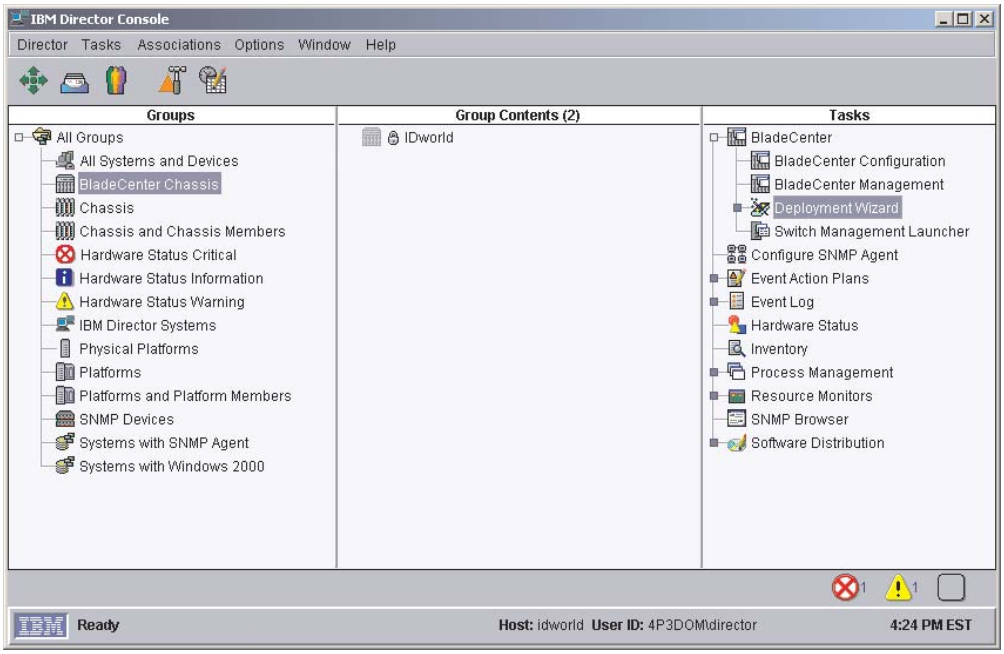

Figure 16. BladeCenter chassis managed object displayed in IBM Director Console

Manually creating a BladeCenter chassis managed object

If the BladeCenter chassis is on a remote network, IBM Director cannot discover the BladeCenter chassis automatically. You must manually create the BladeCenter chassis managed object before you can run the BladeCenter Deployment wizard.

Complete the following steps to manually create a BladeCenter chassis managed object:

1. Manually change the IP address of the management module, if it is set to the default non-routable IP address. For instructions, see “Manually changing the IP address of the BladeCenter chassis” on page 30.

2. From IBM Director Console, right-click on white space in the Group Contents pane. A menu opens.
3. Click **New → BladeCenter Chassis**. The Add BladeCenter Chassis window opens.

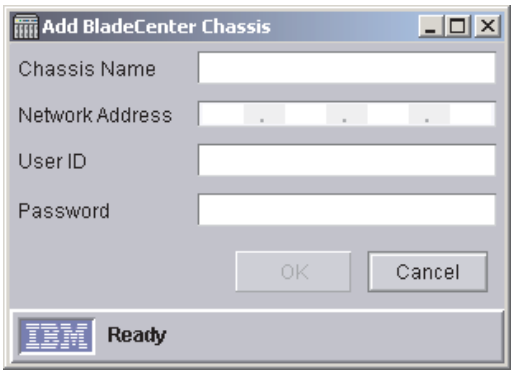

Figure 17. Add BladeCenter Chassis window

4. In the **Chassis Name** field, type a name to identify the chassis. This name is displayed in the Groups pane of IBM Director Console.
5. In the **Network Address** field, type the IP address of the external port of the BladeCenter management module.
6. In the **User ID** field, type a valid user ID for the management module.
7. In the **Password** field, type the password that corresponds to the user ID you typed in step 6.
8. 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 manually change the IP address of the BladeCenter chassis:

1. Cable 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 and press Enter:

   `http://192.168.70.125`

   A password window opens.
5. In the appropriate fields, type the default user name (`USERID`) and password (`PASSW0RD`) for the BladeCenter management module.

   Note: Use uppercase letters and substitute a zero for the “O” in “PASSWORD.”
6. Click **OK**. The BladeCenter Management Module window opens.
7. Click **Continue**. The System Status Summary window opens.
8. In the left pane, under MM Control, click **Network Interfaces**. The Management Module Network Interfaces window opens.

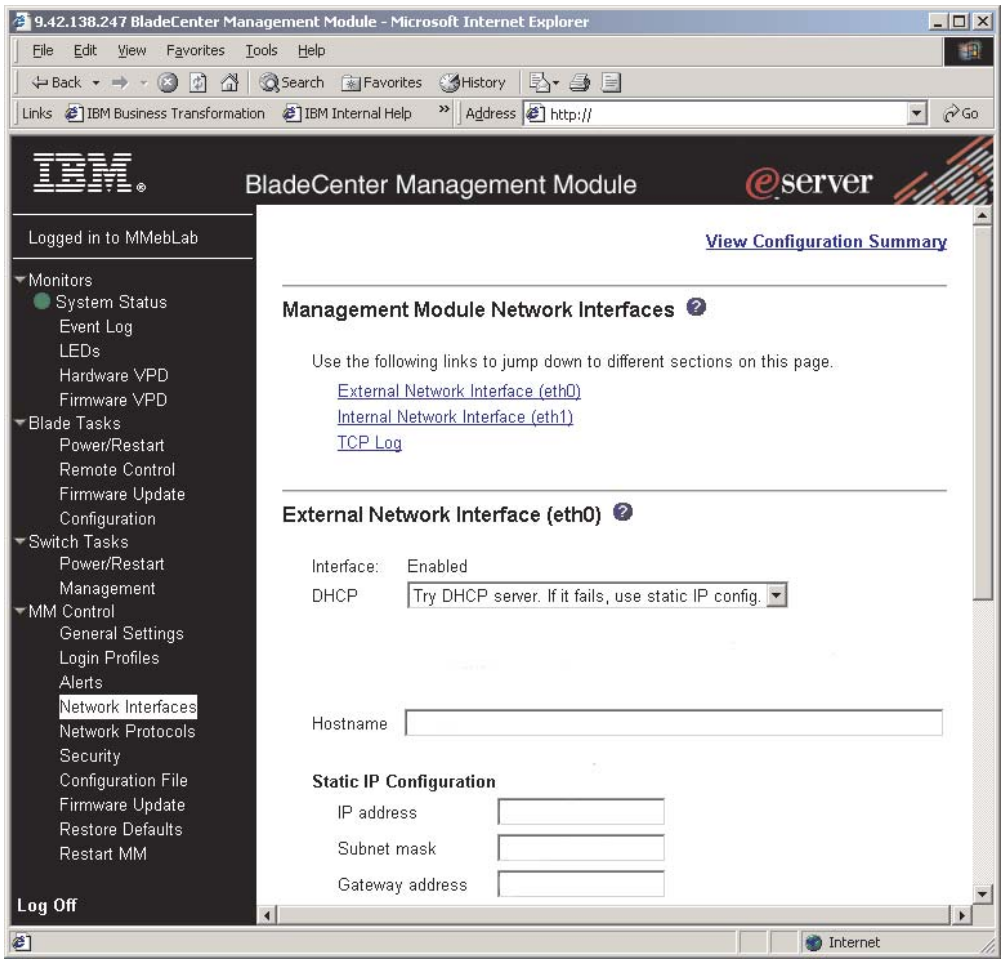

Figure 18. Management Module Network Interface window

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** and **Gateway address** fields, type IP addresses for the subnet mask and network gateway.
12. Click **Save**.
13. In the left pane, under MM Control, click **Restart MM**.

Using the BladeCenter Deployment wizard

You can use the BladeCenter Deployment wizard to complete the following tasks:

- Configure a BladeCenter chassis, including setting up security profiles (user name and password), enabling network protocols, and assigning IP addresses for both the BladeCenter management modules and switch modules.
- Create a reusable profile that can be used to automatically configure new BladeCenter chassis when they are added to the IBM Director environment.

Notes:

1. In order to use the BladeCenter Deployment wizard, IBM Director 4.0 must have created a managed object for the BladeCenter chassis.

2. 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 configure a BladeCenter chassis:

1. In the IBM Director Console Tasks pane, expand the BladeCenter tree.
2. Drag the **Deployment Wizard** task onto the BladeCenter chassis that you want to configure. The BladeCenter Deployment wizard starts and the "Welcome to the BladeCenter Deployment wizard" window opens.

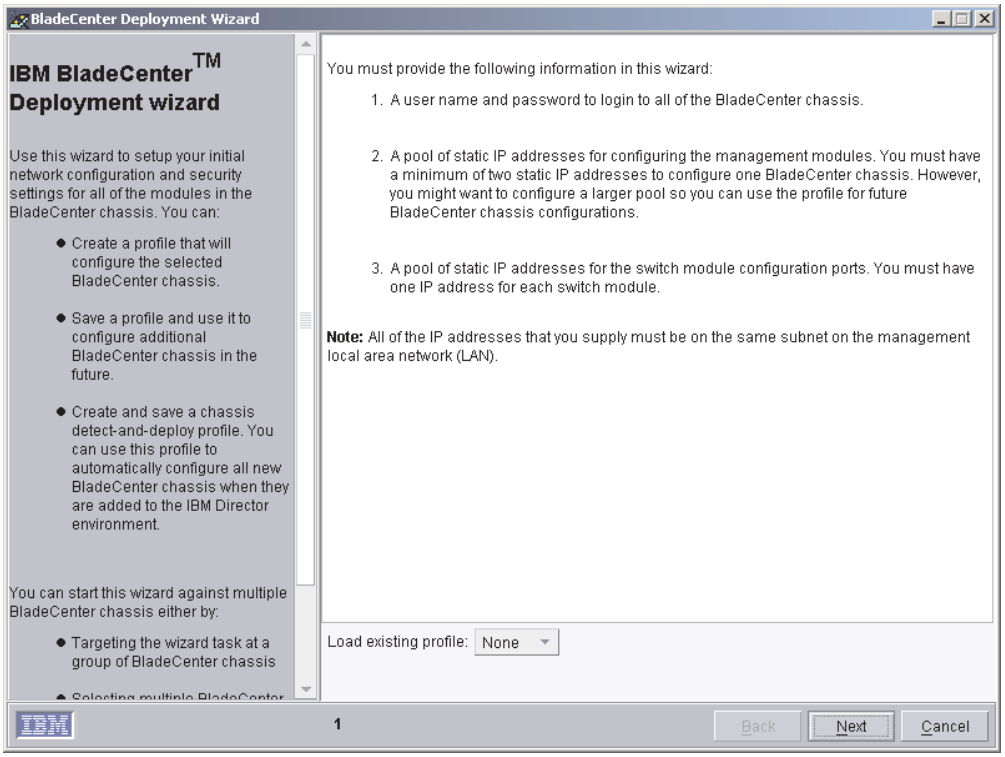

Figure 19. BladeCenter Deployment wizard: "Welcome to the BladeCenter Deployment wizard" window

3. Click **Next**. The "Login to the BladeCenter management module" window opens.

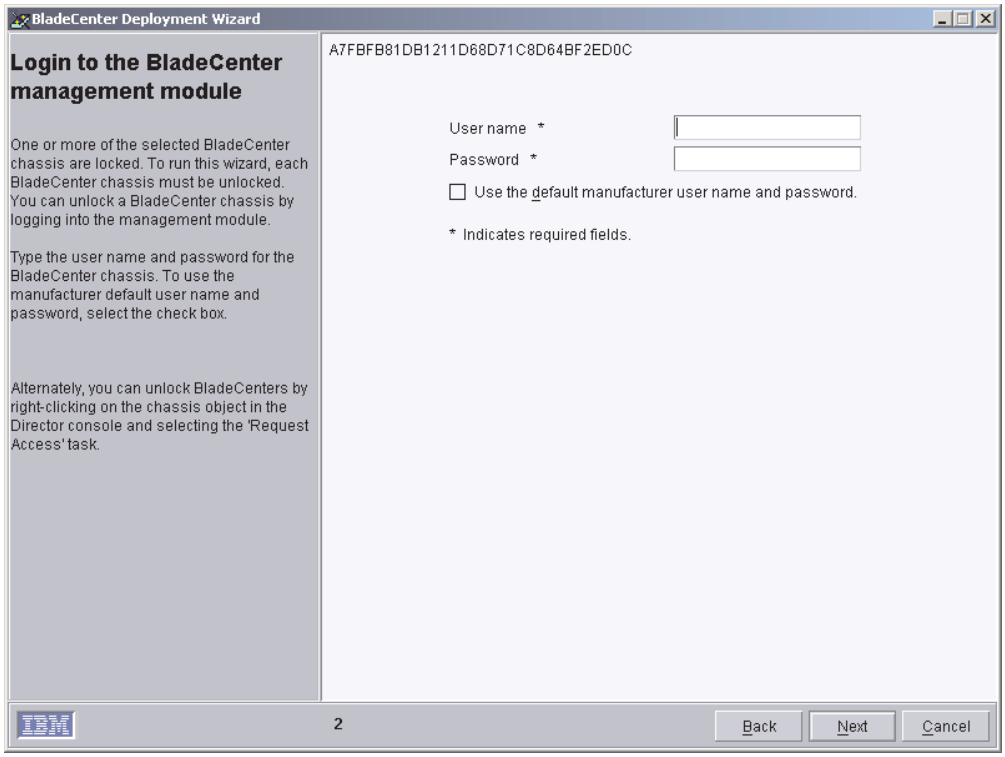

Figure 20. BladeCenter Deployment wizard: "Login to the BladeCenter management module" window

4. If you have not yet changed the default user name and password for the management module, select the **Use the default manufacturer user name and password** check box and go to step 6. Otherwise, go to step 5.
5. In the **User name** field, type a valid user name for an account on the management module.

   In the **Password** and **Confirm password** fields, type the password that corresponds to the user name you typed in step 4.
6. Click **Next**. The "Change user name and password for the management module" window opens.

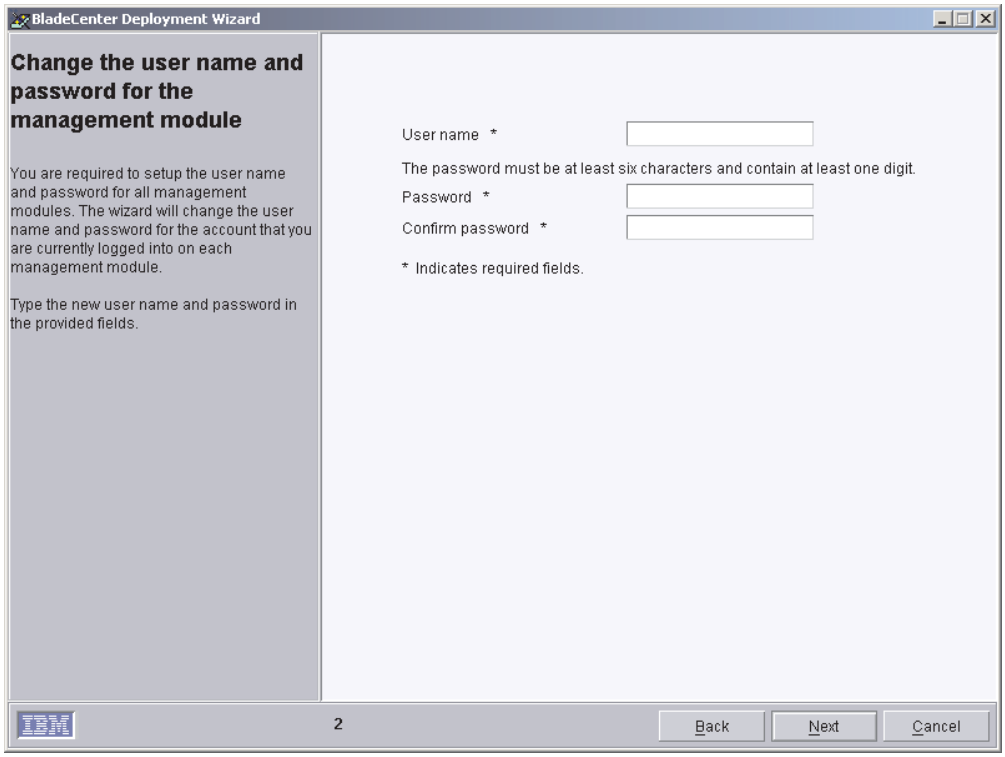

Figure 21. BladeCenter Deployment wizard: "Change the user name and password for the management module" window

7. If you logged into the management module using the manufacturer default user name and password, change them now. In the **User name** field, type a new user name. In the **Password** and **Confirm password** fields, type a new password. It must be at least six characters and contain at least one digit. This user name and password will be used for all BladeCenter chassis selected.

   If you logged into the management module using an existing management module account, type that user name and password in the entry fields.

   Note: If you modify an existing user name or password, the wizard will save the changes.
8. Click **Next**. The "Configure the management module properties" window opens.

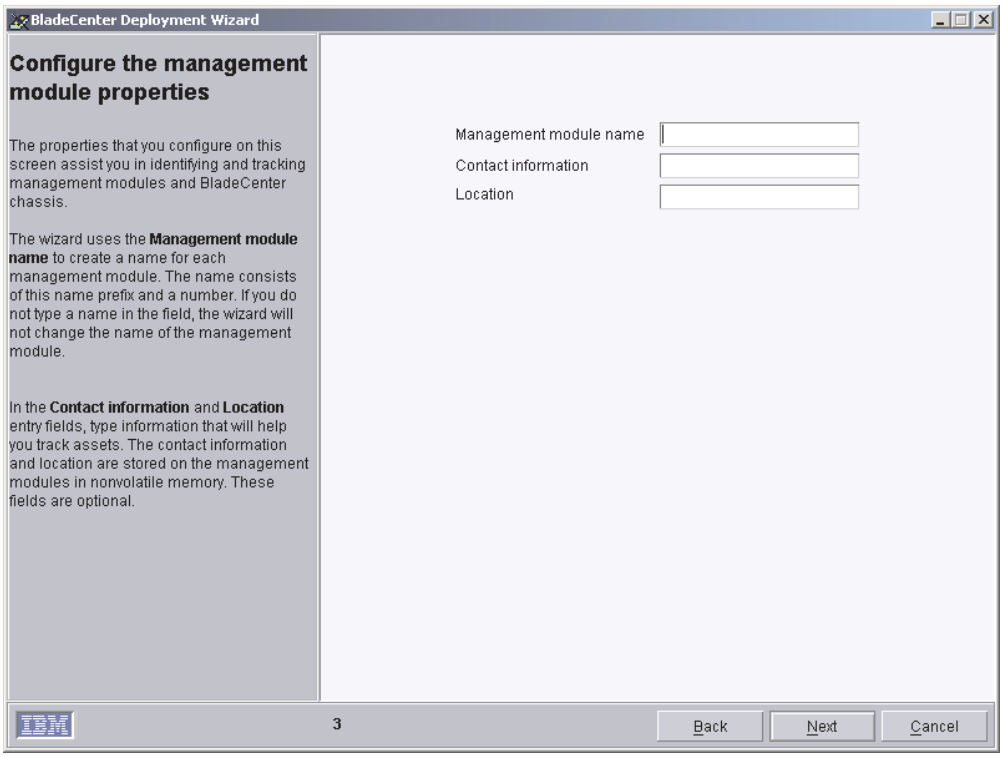

Figure 22. BladeCenter Deployment wizard: "Configure the management module properties" window

9. Complete the following entry fields:

   Management module name
   Type a name for the BladeCenter management module. If you run the BladeCenter Deployment wizard against multiple BladeCenter chassis, the wizard will add a unique number to this string.

   If you leave this entry field blank, the default management module name is MM*xxxxxxxxxxxx*, where *xxxxxxxxxxxx* is the burned-in media access control (MAC) address of the management module.

   Contact information
   Type the name of the asset owner.

   Location
   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.

10. Click **Next**. The "Configure the management module protocols" window opens.

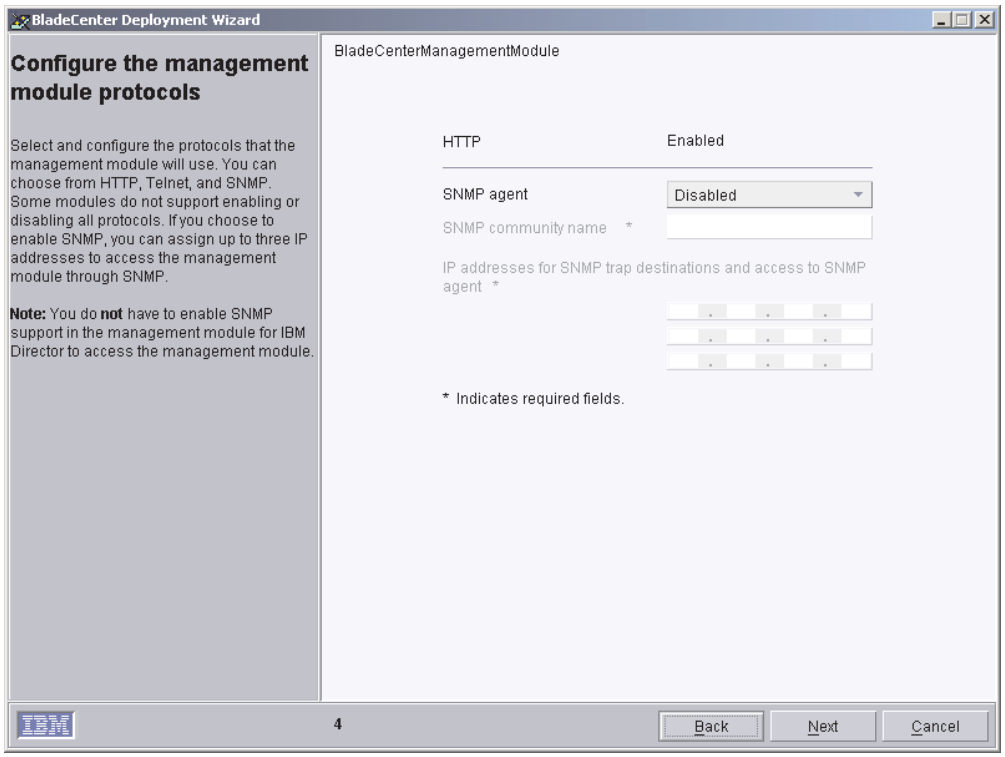

Figure 23. BladeCenter Deployment wizard: "Configure the management module protocols" window

11. Enable the network protocols for the BladeCenter management module.

    If you enable SNMP, you must provide an SNMP community name and at least one IP address. You can assign up to three IP addresses to access the management module through SNMP.

    Note: To enable SNMP on the management module, you *must* have typed information in the **Contact information** and **Location** entry fields on the previous window. Click **Back** to return to the "Configure the management module properties" window.

12. Click **Next**. The "Configure the IP settings" window opens.

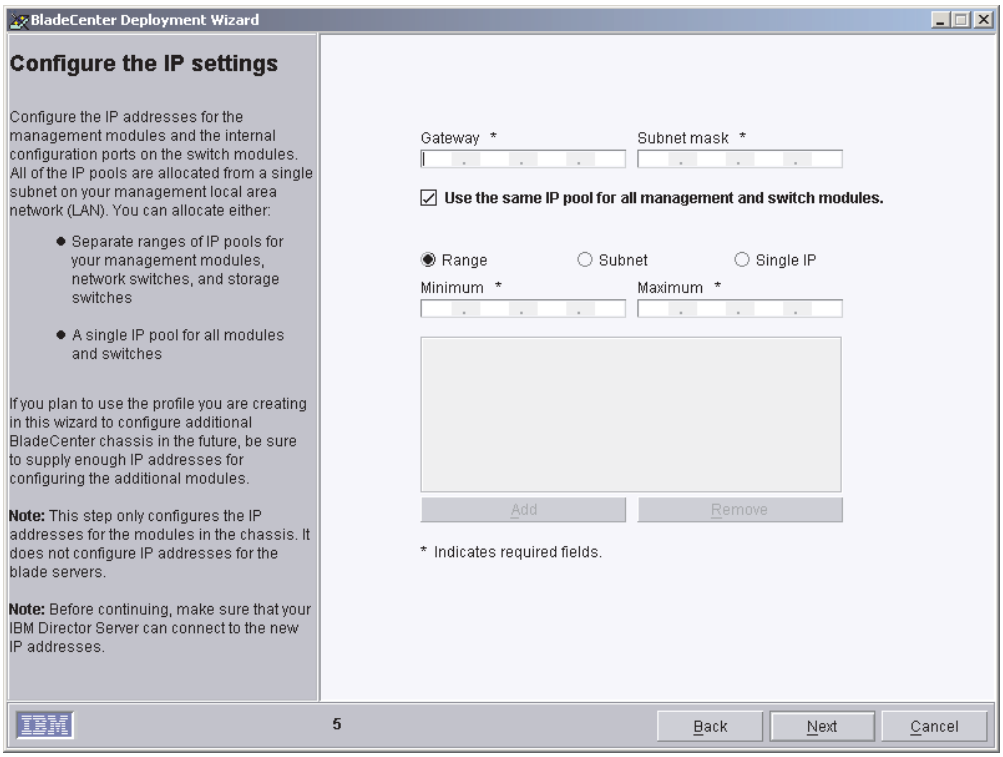

Figure 24. BladeCenter Deployment wizard: "Configure the IP settings" window

13. In the **Gateway** field, enter the IP address for the network gateway. In the **Subnet mask** field, enter the IP address for the subnet mask.
14. To configure separate pools of IP addresses for the management modules and switch modules, go to step 17. Otherwise, select the **Use the same IP pool for all management and switch modules** check box.
15. Create a pool of IP addresses. You can add IP addresses to the pool in the following ways:

    Individual

    Click **Single IP**. In the **IP address** field, type the IP address; then, click **Add**.

    Subnet

    Click **Subnet**. In the **Network gateway** field, type the IP address for the network gateway. In the **Subnet mask** field, type the IP address for the subnet mask. Click **Add**.

    Range

    Click **Range**. In the **Minimum** and **Maximum** fields, type the IP addresses that specify the range. Click **Add**.
16. When you have finished creating the pool of IP addresses for the management modules and switch modules, go to step 18 on page 38.
17. Clear the **Use the same IP pool for all management and switch modules** check box; the **Management Module** and **Network Switch Module** tabs are displayed.
    a. To create the pool of IP addresses for the management modules, click **Management Module** and follow the instructions outlined in step 15.
    b. To create the pool of IP addresses for the switch modules, click **Network Switch Module** and follow the instructions outlined in step 15.

18. Click **Next**. The “Change the user name and password for switch modules” window opens.

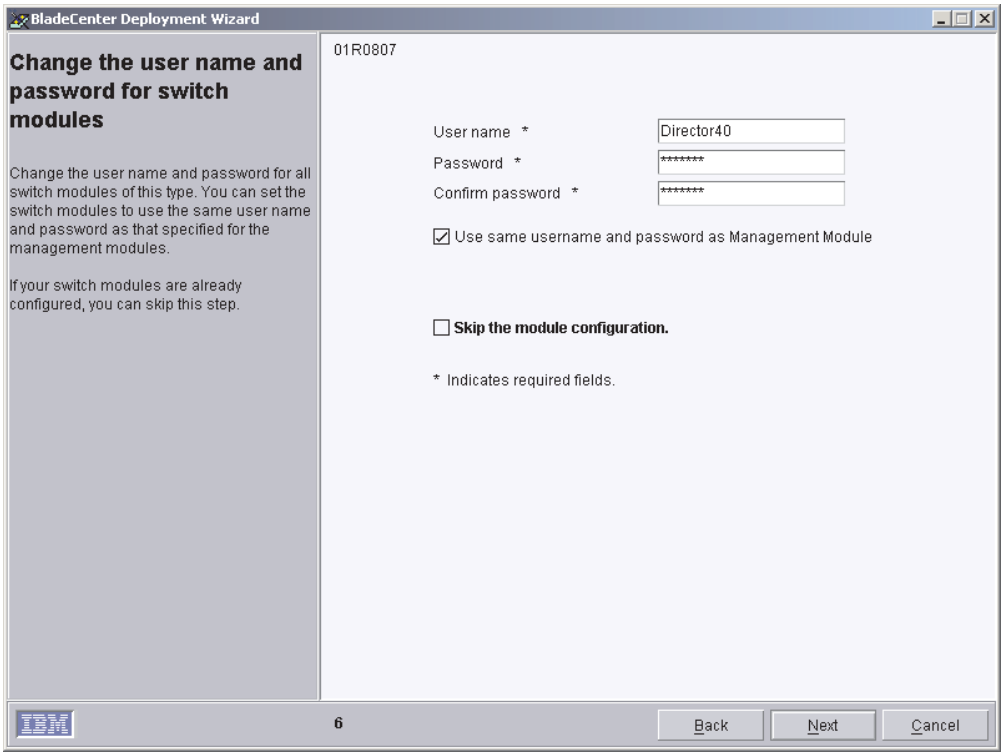

Figure 25. BladeCenter Deployment wizard: “Change the user name and password for switch modules” window

19. If you want to use the same user name and password for both the BladeCenter management modules and switch modules, select the **Use the same username and password as Management Module** check box. Go to step 20.

    If the switch modules are already configured, select the **Skip the module configuration** check box. Go to step 20.

    If you want to change the user name and password for all BladeCenter switch modules of this specific type, complete the following steps:

    a. In the **User name** field, type the new user name.

    b. In the **Password** and **Confirm password** fields, type the new password.

20. Click **Next**. The “Configure the switch module” window opens.

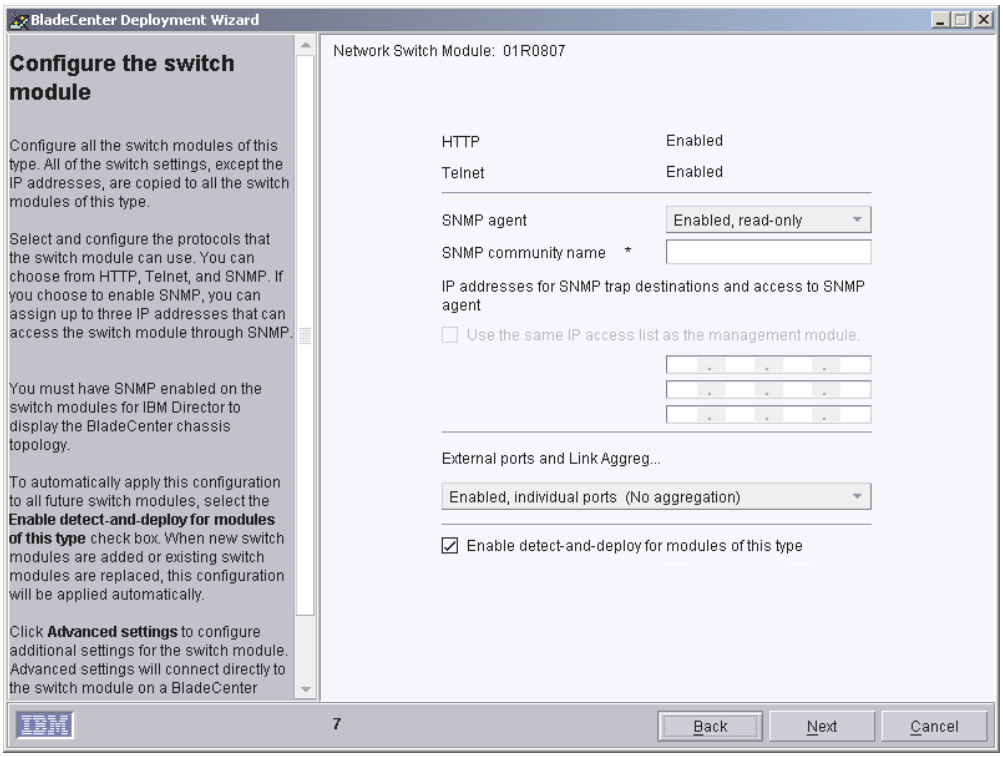

Figure 26. BladeCenter Deployment wizard: "Configure the switch module"' window

21. Enable network protocols for all BladeCenter switch modules of this type.

    If you enable SNMP, you must provide an SNMP community name and at least one IP address. You can assign up to three IP addresses. If you want to use the same pool of IP addresses as that used for the management module, select the **Use the same IP access list as the management module** check box.

    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.

22. In the **External ports and link aggregation** list, click the option that indicates how you want to configure the external ports. They can be aggregated into either one or two link aggregation groups (trunks), enabled without aggregation, or disabled.

    Note: Before you configure the external ports as link aggregation groups, verify that the LAN switch has a compatible multi-port trunk configuration.

23. Click **Next**. The "Deploy the operating system" window opens.

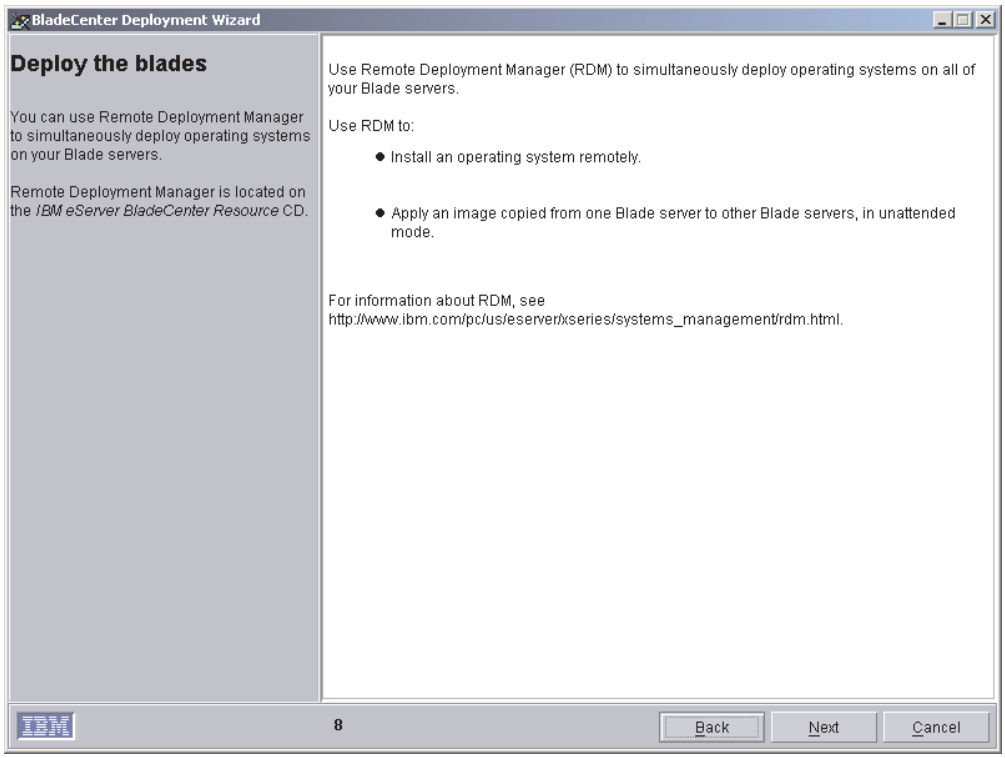

Figure 27. BladeCenter Deployment wizard: "Deploy the operating system" window

24. Click **Next**. The "Setup summary" window opens.

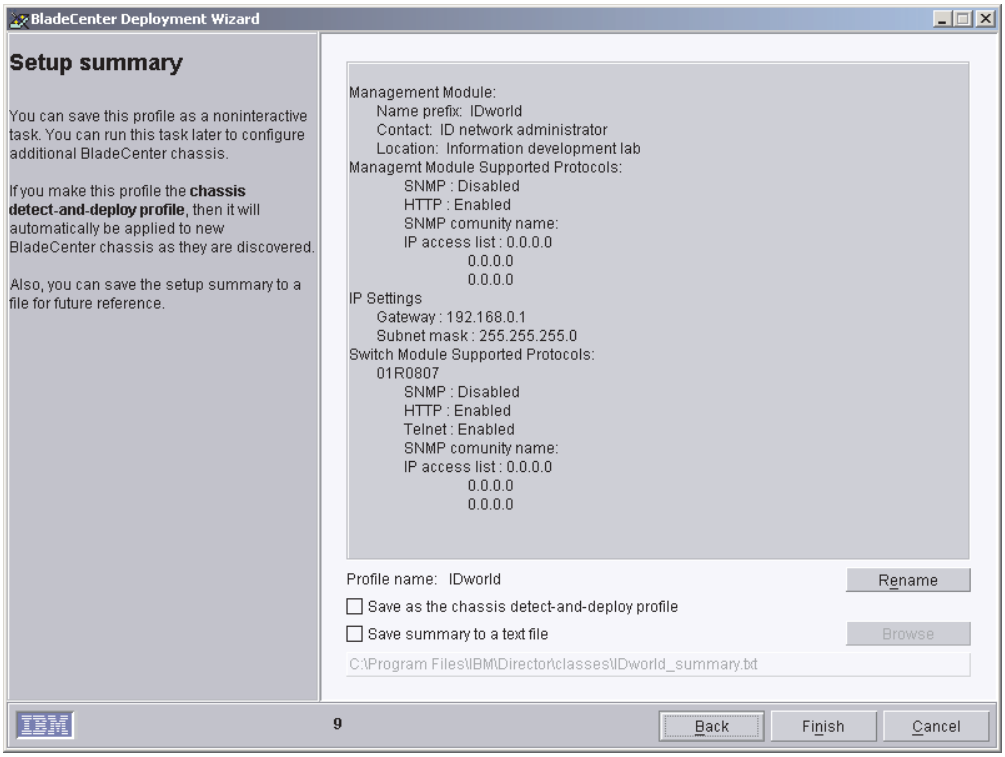

Figure 28. BladeCenter Deployment wizard: "Setup summary" window

25. A summary of the configuration options selected is displayed in the right pane.

    By default, the profile is given the name you assigned to the management module. To change it, click **Rename** and assign a new name to this profile.

    To make this profile the default profile, select the **Save this profile as the chassis detect-and-deploy profile** check box. This profile will be applied to all new BladeCenter chassis automatically when they are discovered by IBM Director 4.0.

    Note: There can be only one default profile. If a default profile already exists and you select the **Save this profile as the default profile** check box, you will overwrite the existing profile.

    To save the setup summary for future reference, select the **Save summary to a text file** check box.

26. Click **Finish**. The profile is created. It appears as a subtask under Deployment wizard in the Tasks pane of IBM Director Console.

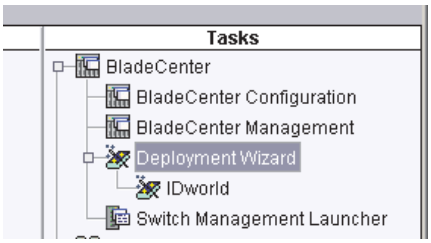

Figure 29. BladeCenter Deployment wizard: Sample profile task

27. When prompted, select when you want to run the profile. You can choose to run the profile now, schedule a task, or cancel.

Chapter 6. Installing IBM Director Agent

After you have installed the operating systems on the blade servers, install IBM Director Agent.

Installing IBM Director Agent on Microsoft Windows

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:

1. Insert the *IBM Director 4.0* 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 **Install IBM Director Agent**. The InstallShield wizard starts, and the Welcome to the InstallShield Wizard window opens.
6. Click **Next**. The License Agreement window opens.
7. Click **I accept the terms of the license agreement** and click **Next**. The "Feature and installation directory selection" window opens.

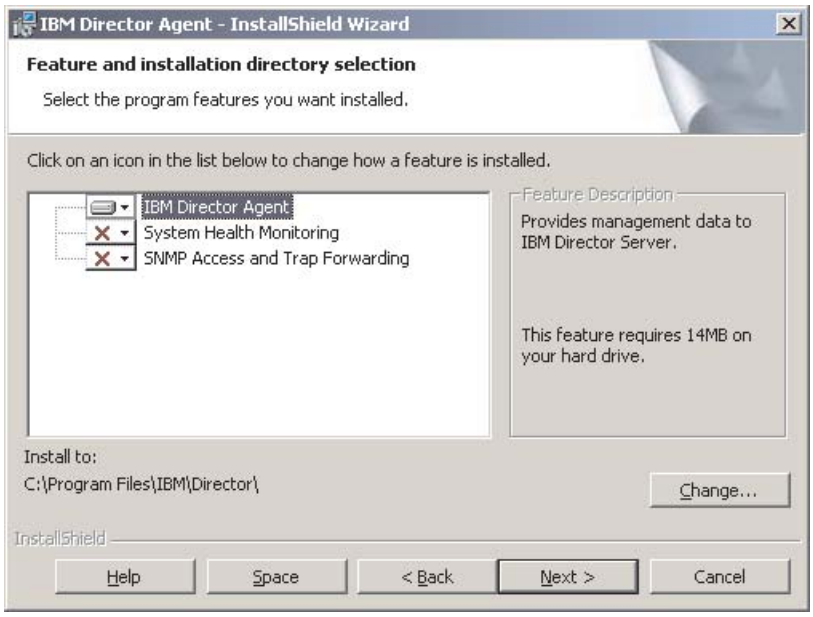

Figure 30. Installing IBM Director Agent: "Feature and installation directory selection" window

IBM Director Agent is automatically selected for installation; a hard disk icon  is displayed to the left of the component.  is displayed to the left of the optional features.

You can install the following optional features:

System Health Monitoring
Monitors the status of hardware components; produces and relays hardware alerts.

SNMP Access and Trap Forwarding
Enables access to managed-system data and alerts through SNMP.

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

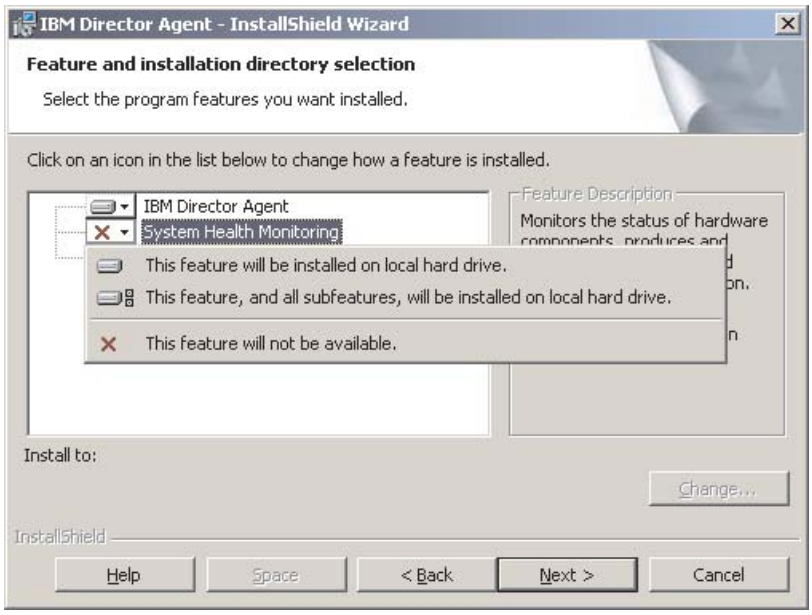

Figure 31. Installing IBM Director Agent: "Feature and installation directory selection" window

9. To install the feature, click **This feature will be installed on local hard drive** or **This feature, and all its subfeatures, will be installed on local hard drive**.
10. Click **Next**. The "Software-distribution settings" window opens.

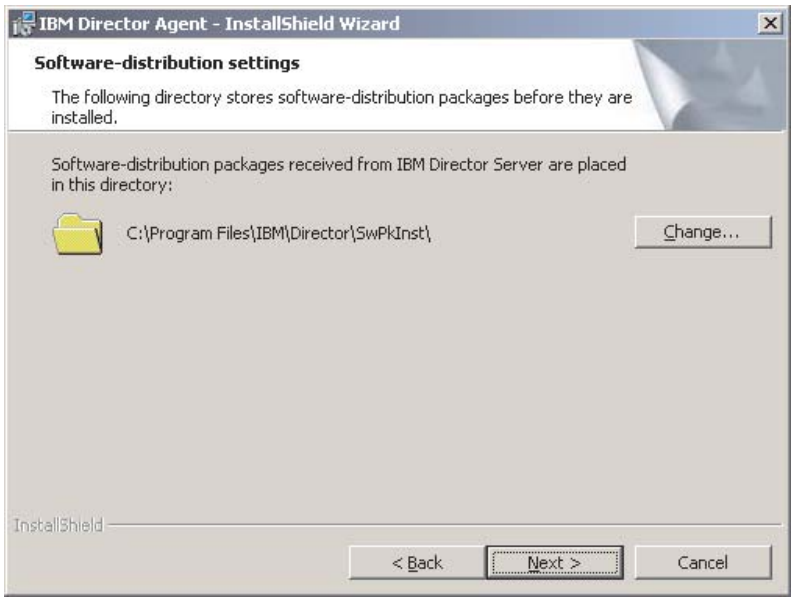

Figure 32. Installing IBM Director Agent: "Software-distribution settings" window

11. To select an alternate location for where software-distribution packages are stored before being applied to IBM Director Agent, click **Change** and select another directory.
12. Click **Next**. The Ready to Install the Program window opens.
13. Click **Install**. The Installing IBM Director Agent window opens.

    The status bar displays the progress of the installation. When the installation is completed, the "Network driver configuration" window opens.

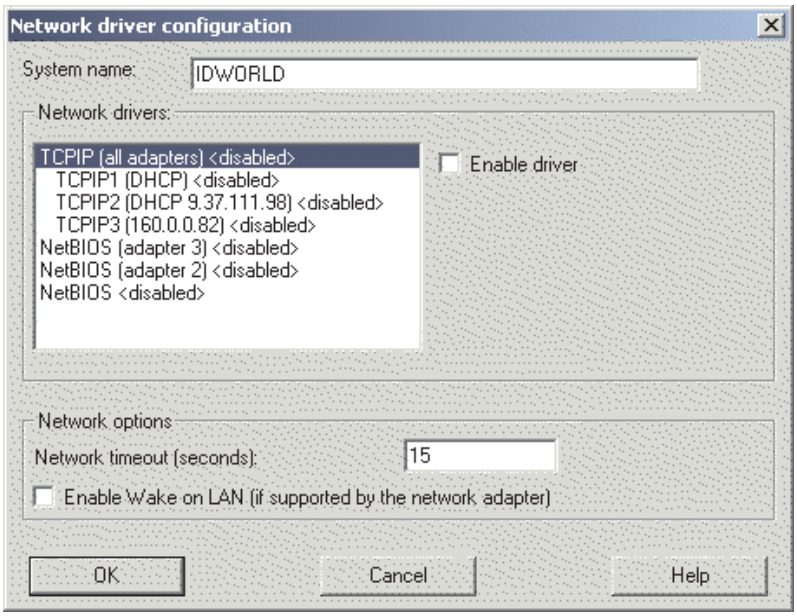

Figure 33. Installing IBM Director Agent: "Network driver configuration" window

14. In the **System name** field, type the name that you want displayed in IBM Director Console. By default, this is the NetBIOS name of the managed system.

15. In the **Network timeout** field, type the number of seconds that IBM Director Server will wait for a response from IBM Director Agent. By default, this is set for 15 seconds.

    To enable a network driver, select the communication protocol that you are using in your network (such as TCP/IP or NetBIOS) and select the **Enable driver** check box.

    Select the **Enable Wake on LAN** check box if the network adapter supports the Wake on LAN feature.

    Note: To determine whether your system supports Wake on LAN, see your system documentation.

16. Click **OK**.

    The status bar displays the progress of the installation. When the installation is complete, the InstallShield Wizard Completed window opens.

17. Click **Finish**. The IBM Director Agent Installer Information window opens.
18. 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 posed by the InstallShield wizard. A system administrator 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:

1. Insert the *IBM Director 4.0* 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 4.0* 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 4.0* 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. You must restart the operating system after the installation is complete.
     - SILENT suppresses all output to the screen during installation and then restarts the operating system.
   - *responsefile.rsp* is the path and name of the response file that you created in step 5.

8. If you issued the UNATTENDED command in step 7, restart the operating system when prompted to do so.
9. Remove the CD from the CD-ROM drive.

Installing IBM Director Agent on Linux

Note: Before installing IBM Director Agent, verify that the operating-system password encryption method is set to MD5 (message digest 5).

Complete the following steps to install IBM Director Agent:

1. Insert the *IBM Director 4.0* 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/agent/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 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 /destinationdirectory/dirinstall
   ```

   where *destinationdirectory* 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 and choose log file options.
8. Save the modified installation script.
9. To install IBM Director, type the following command and press Enter:

   ```
   /destinationdirectory/dirinstall
   ```

   where *destinationdirectory* is the local directory to which you copied the installation script.
10. When the installation is complete, start IBM Director Agent. Type the following command and press Enter:

    ```
    /opt/IBM/director/bin/twgstart
    ```
11. 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.

12. Remove the CD from the CD-ROM drive.

After IBM Director Agent is installed, you can enable Wake on LAN. See “Enabling Wake on LAN” on page 66.

Chapter 7. Configuring IBM Director

This chapter provides information about using the Event Action Plan wizard, setting discovery preferences, discovering the blade servers, and authorizing IBM Director users.

Using the Event Action Plan wizard

Important:

If your IBM Director environment includes managed systems running IBM Director Agent 3.x, *do not* use the Event Action Plan wizard to initiate discovery. Instead, set your discovery preferences to ensure that only the blade servers are discovered. Then, apply the event action plan to the blade servers *only*.

The Event Action Plan wizard will start every time you log into 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 the above actions, you will no longer be 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 4.0 for BladeCenter products 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 60.

To use the Event Action Plan wizard, complete the following tasks:

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

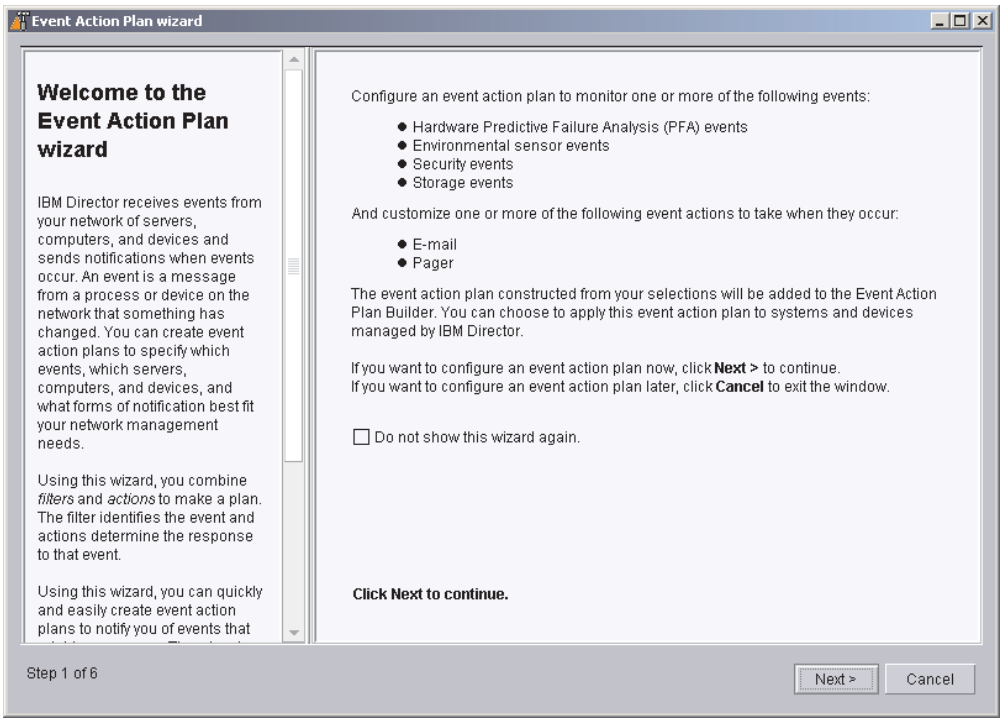

Figure 34. Event Action Plan wizard: "Welcome to the Event Action Plan wizard" window

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

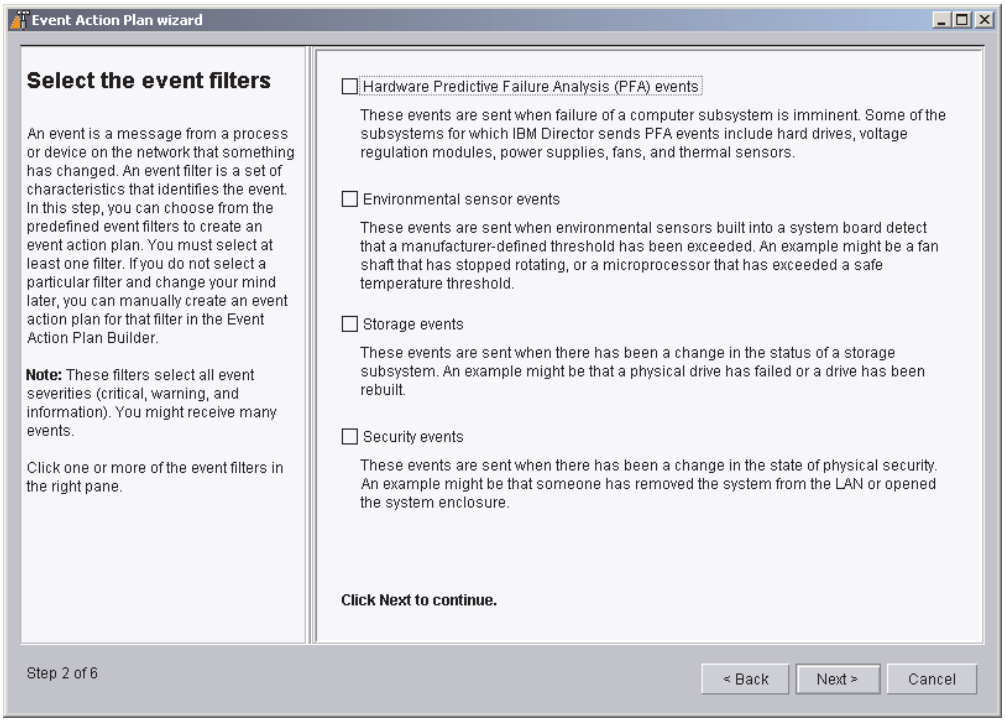

Figure 35. Event Action Plan wizard: "Select the event filters" window

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 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.

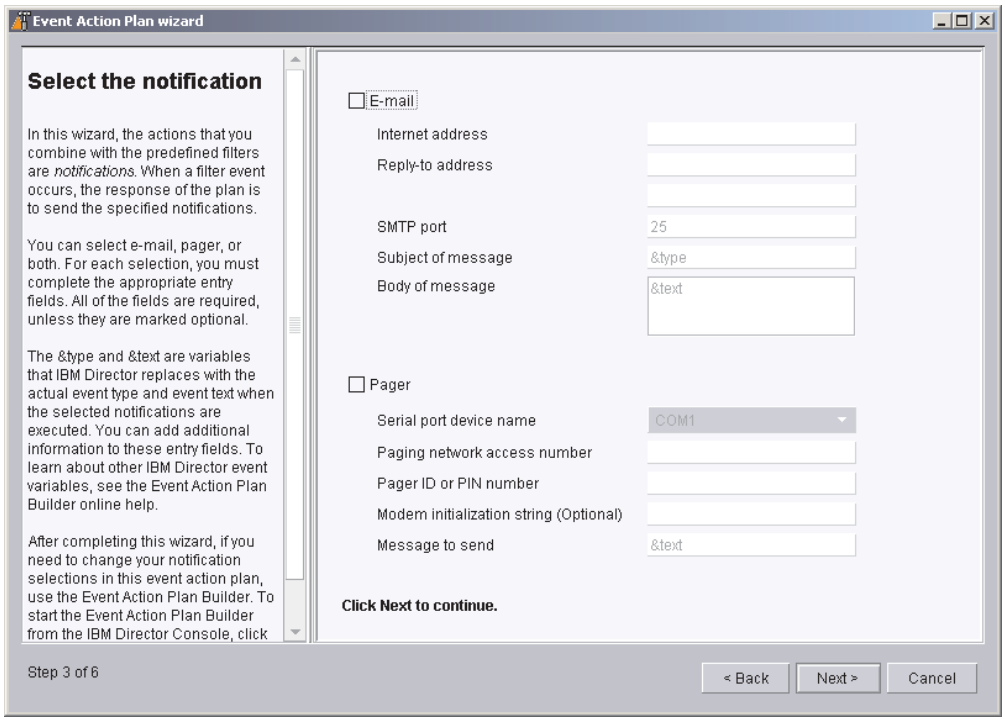

Figure 36. Event Action Plan wizard: “Select the notification” window

5. If you want to be notified by e-mail when an event occurs, select the **E-mail** check box. Then complete the following entry fields:

   Internet address
   Type the e-mail address to which the notification will be sent.

Reply-to address
Type the e-mail address that will be displayed in the reply-to field of the e-mail.

SMTP port
Type the port number of the SMTP server. By default, the SMTP port is set to 25.

Subject of message
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.”

Body of message
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 such an e-mail is generated, the body will contain the time and date the event occurred, as well as details about the event.

“&type,” “&system,” “&time,” “&date,” and “&text” are event substitution variables. For information about other event data substitution variables, see the *IBM Director 4.0 for BladeCenter products Systems Management Guide*.

6. If you want to be notified by pager, select the **Pager** check box. Then complete the following entry fields:

   Serial port device name
   Click the name of the serial port device.

   Paging network access number
   Type the telephone number that will be dialed when an event occurs.

   Pager ID or PIN
   Type the pager ID or personal identification number (PIN).

   Modem initialization string (Optional)
   Type the modem initialization string.

   Message to send
   Type the message that will be sent when an event occurs.

7. Click **Next**. The “Apply the event action plan” window opens.

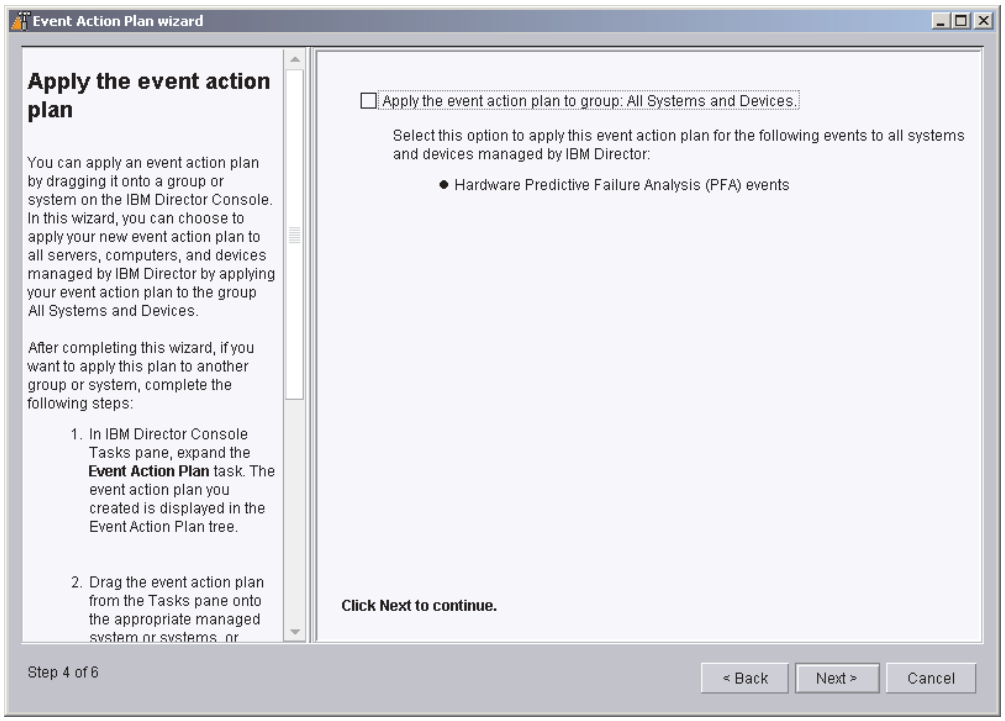

Figure 37. Event Action Plan wizard: "Apply the event action plan" window

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.

   Note: If your environment includes managed systems running IBM Director Agent 3.x, *do not* 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.

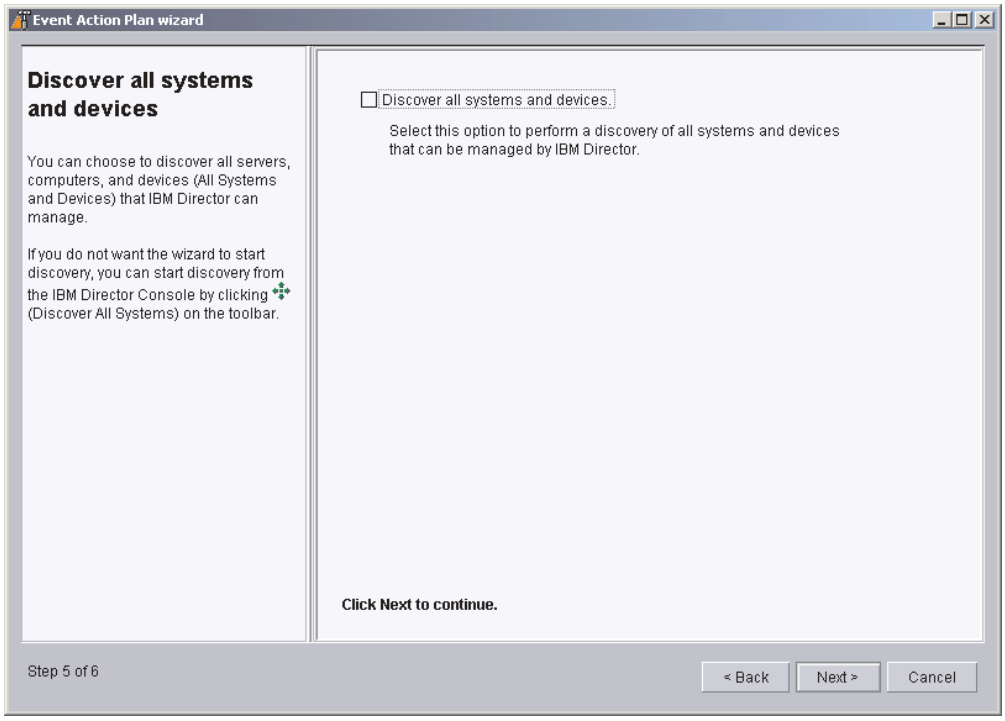

Figure 38. Event Action Plan wizard: "Discover all systems and devices" window

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.

    Note: If your environment includes managed systems running IBM Director Agent 3.x, *do not* select the **Discover all systems and devices** check box.

11. Click **Next**. The "Review your selection summary" window opens.

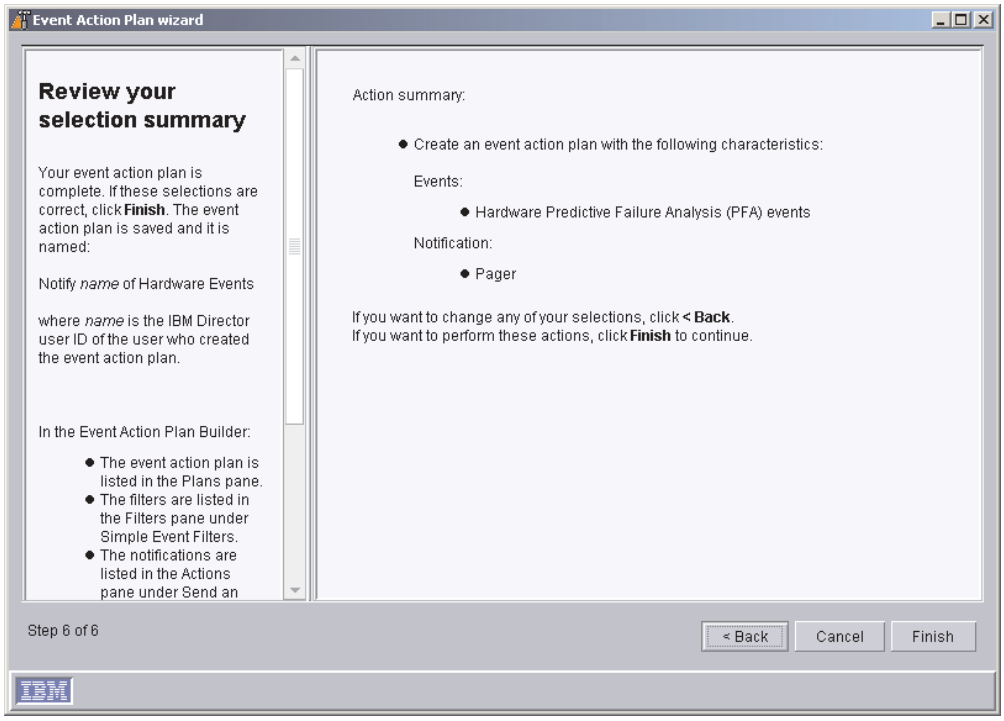

Figure 39. Event Action Plan wizard: "Review your selection summary" window

Review the selections. If you want to change any of your selections, click **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.

Important: If your environment includes managed systems running IBM Director Agent 3.x, configure your discovery preferences to discover blade servers. See "Discovering blade servers only" on page 57. Then, apply the event action plan you created using the Event Action Plan wizard to the blade servers.

Discovery

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.

Types of discovery

IBM Director supports four types of discovery:

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 can also 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.

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 listen on 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 only available 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. To discover certain types of managed systems (for example, dial-up systems), it might be necessary to use Unicast discovery. Unicast discovery is only available for TCP/IP systems.

Note: If your IBM Director environment includes managed systems running IBM Director Agent 3.x, use unicast discovery to ensure that your management server discovers blade servers running IBM Director Agent 4.0 *only*.

Broadcast relay agents

Broadcast relay allows the server to discover TCP/IP and IPX systems when the systems are not directly reachable by broadcast packets due to 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

Important:

If your IBM Director environment includes managed systems running IBM Director Agent 3.x, set your discovery preferences to ensure that only blade servers are discovered. Go to “Discovering blade servers only” on page 57.

Complete the following steps to configure discovery preferences:

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

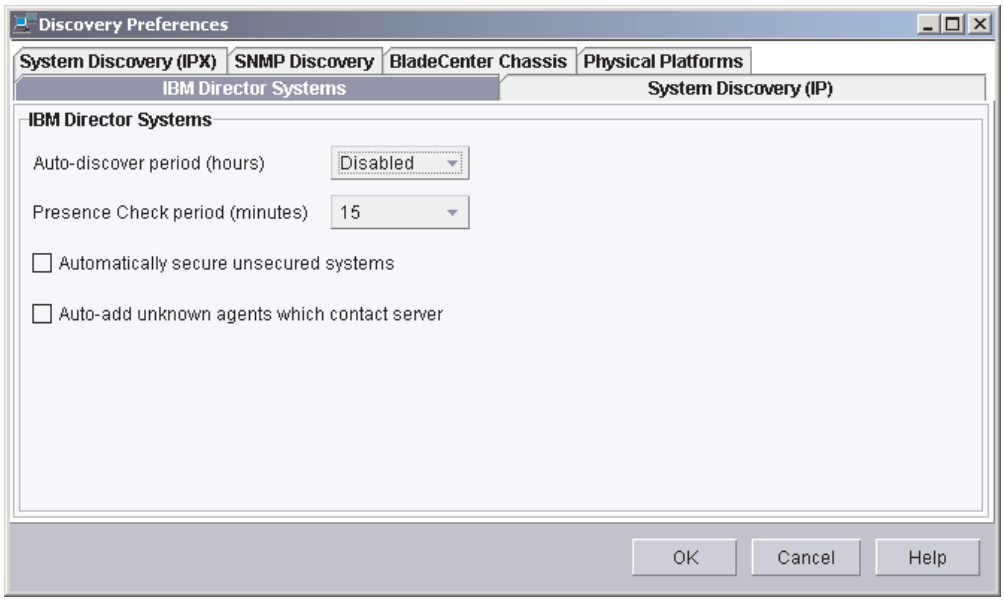

Figure 40. Discovery Preferences window

This window has six different pages:

IBM Director Systems
Sets general discovery preferences

System Discovery (IP)
Defines how IBM Director discovers managed systems reachable through TCP/IP

System Discovery (IPX)
Defines how IBM Director discovers managed systems reachable through IPX

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 appropriate tab. Click **OK** when you have finished configuring discovery preferences.

Discovering blade servers only

Complete the following steps to discover blade servers *only*:

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

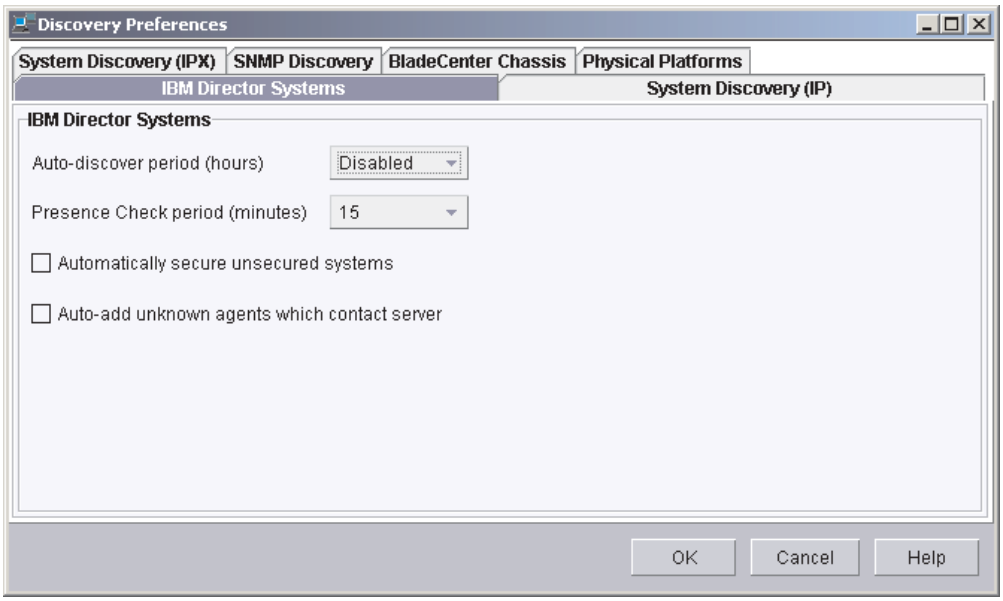

Figure 41. Discovery Preferences window

2. Click **System Discovery (IP)**. The System Discovery (IP) page opens.

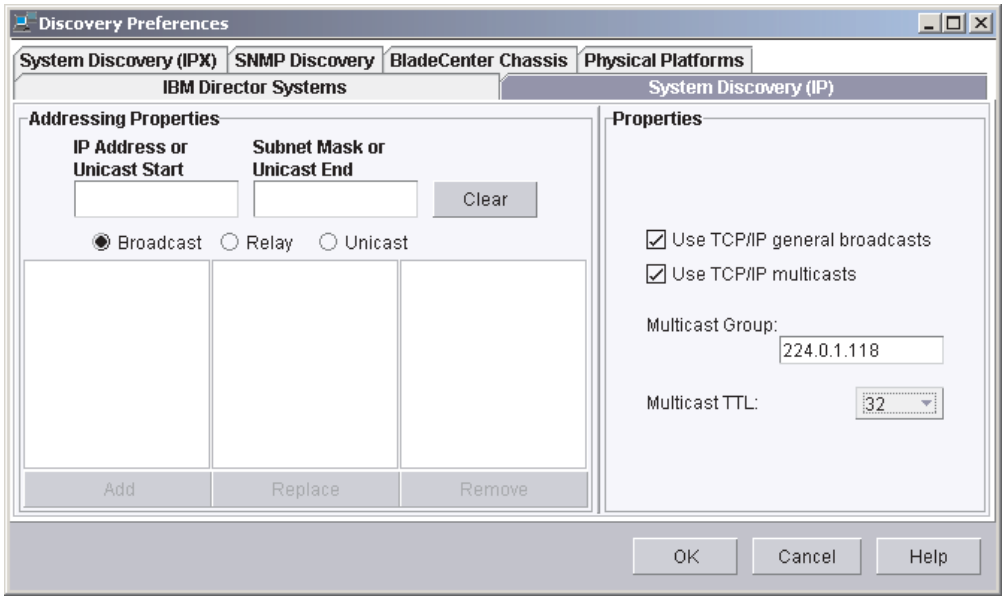

Figure 42. Discovery Preferences window: System Discovery (IP) page

3. In the **Addressing Properties** pane, click **Unicast**.
4. Specify the IP addresses that are assigned to the blade servers. You can add IP addresses individually or you can specify a range.

   To add IP addresses individually, type the IP address in the **IP Address or Unicast Start** field; then, click **Add**. Repeat until you have added all the IP addresses.

   To specify a range of IP addresses, type the beginning address in the **IP Address or Unicast Start** field and the ending address in the **Subnet Mask or Unicast End** field. Click **Add**.

5. In the Properties pane, clear the **Use TCP/IP general broadcasts** and **Use TCP/IP multicasts** check boxes.
6. Click the **SNMP Discovery** tab. The SNMP Discovery page opens.

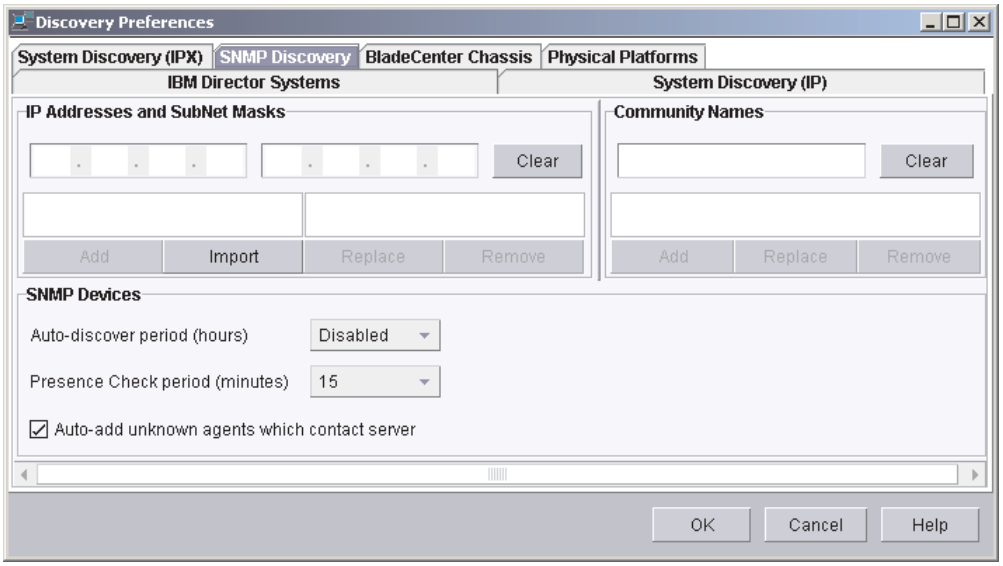

Figure 43. Discovery Preferences window: SNMP Discovery page

7. Clear the **Auto-add unknown agents which contact server** check box.
8. Click **OK**. The Discovery Preferences window closes.
9. To discover the blade servers, click **Tasks → Discover Systems → IBM Director Systems**.

Authorizing IBM Director users

IBM Director Console uses the underlying operating-system user accounts for user-logon security. When a user logs into 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 *and* be a member of either the DirAdmin or DirSuper group. When IBM Director Server is installed, these two groups are automatically created on the underlying operating system. Members of the DirAdmin group have basic administrative privileges in the IBM Director environment, while members of the DirSuper group have super user privileges.

Once logged into IBM Director, users' ability to perform tasks depends on what access privileges they have been granted in the IBM Director environment. You can configure a default set of privileges for all user accounts, and you can edit user accounts on an individual basis.

Creating user account defaults

You can use the User Defaults Editor to set the default access privileges for all IBM Director user accounts. Complete the following steps to create user account defaults:

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

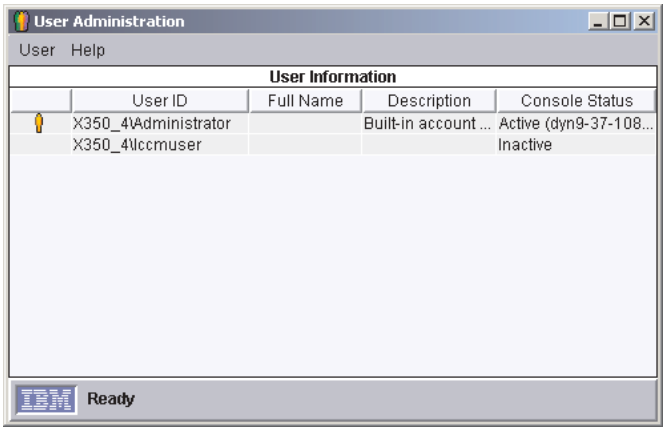

Figure 44. User Administration window

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

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

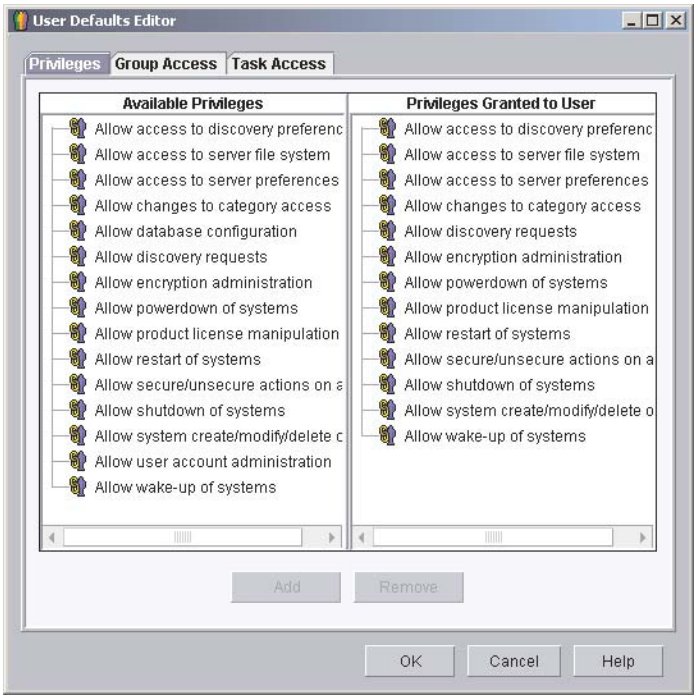

Figure 45. User Defaults Editor window

3. Set the default access privileges for all IBM Director users.

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.

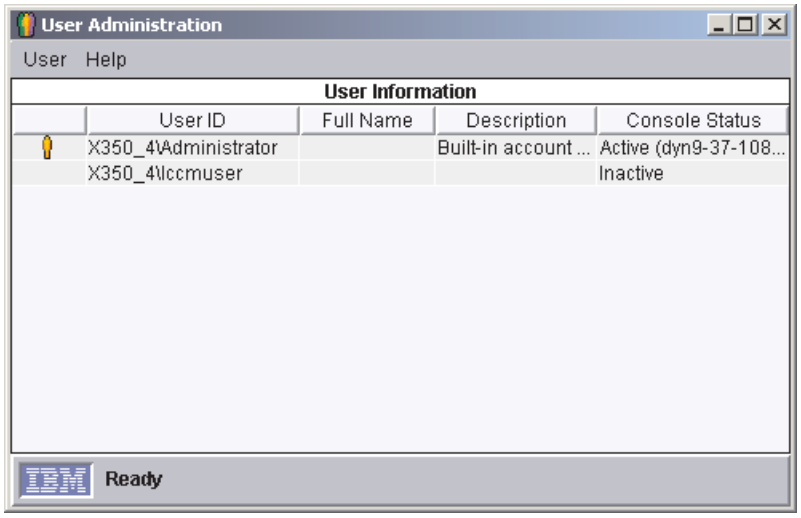

Figure 46. User Administration window

   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.

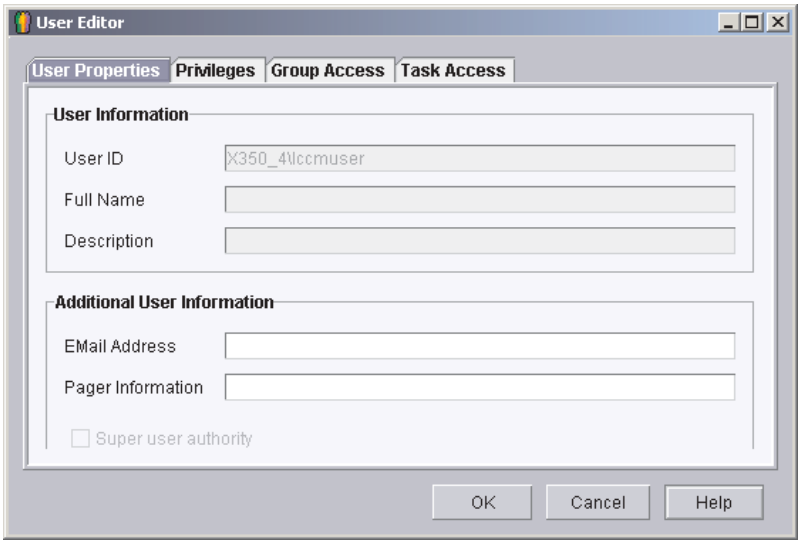

Figure 47. User Editor window: User Properties page

3. Click the **Privileges** tab. The Privileges page opens.

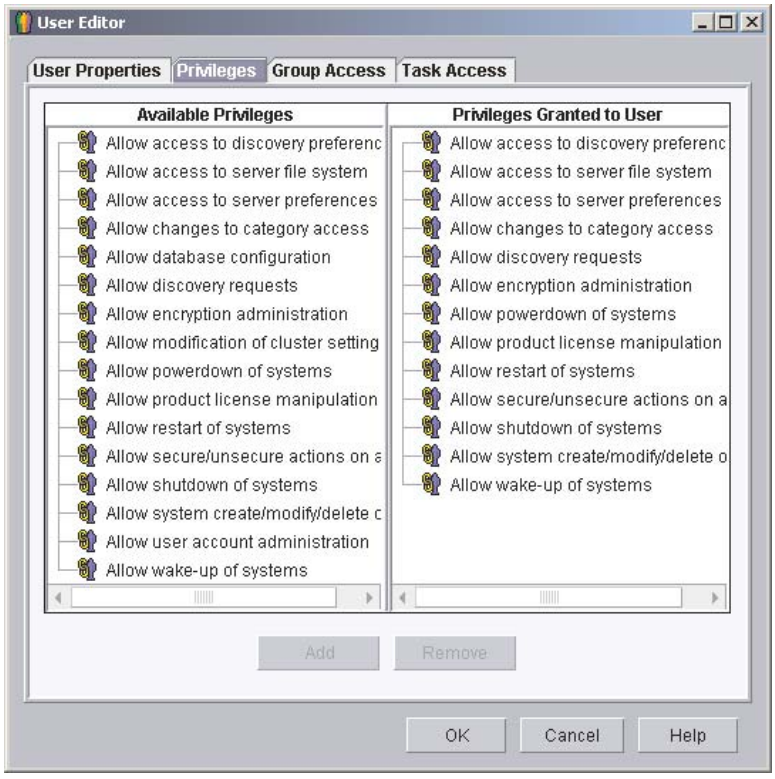

Figure 48. User Editor window: Privileges page

4. To add a privilege, click on the privilege in the **Available Privileges** pane and then click **Add**.

   To remove a privilege, click on 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 opens.

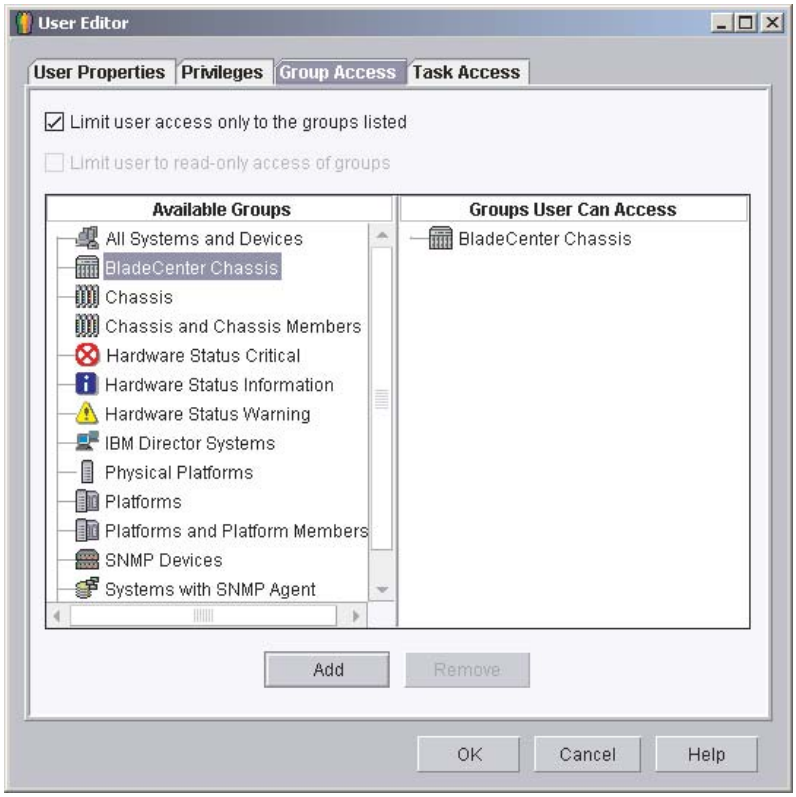

Figure 49. User Editor window: Group Access page

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 opens.

Figure 50. 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.

Chapter 8. Modifying and uninstalling IBM Director

This chapter provides instructions for modifying and uninstalling IBM Director.

Modifying IBM Director running on Windows

After you install IBM Director, you can modify the installation. You can install the IBM Director database, install a new feature, or remove a feature.

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. Stop the IBM Director Support Service. 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.
4. When the database installation is complete, restart the IBM Director Support Service. Type the following command and press Enter:

   ```
   net start twgipc
   ```

Installing or uninstalling an IBM Director feature

Complete the following steps to add or remove a feature:

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 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 51. Program Maintenance window

5. Click **Modify**; then, click **Next**.
6. Continue through the wizard, making changes as necessary.

Modifying IBM Director Agent running on Linux

After you install IBM Director Agent, you can enable Wake on LAN, install a previously uninstalled feature, or remove a feature.

Enabling Wake on LAN

Complete the following steps to enable Wake on LAN:

1. Stop IBM Director Agent. 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 located in /opt/IBM/director/data.
3. Modify the value of ipc.wakeonlan to read as follows:
   `ipc.wakeonlan=1`
4. Save and close the ServiceNodeLocal.properties file.
5. Start IBM Director Agent. Type the following command and press Enter:
   `/opt/IBM/director/bin/twgstart`

Installing an IBM Director feature

Complete the following steps to install a previously uninstalled feature:

1. Modify the dirinstall script. This file is located in the IBM/director/bin directory.
2. Stop IBM Director Agent. Type the following command and press Enter:
   `/opt/IBM/director/bin/twgstop`
3. Run the dirinstall script.
4. Start IBM Director Agent. Type the following command and press Enter:
   `/opt/IBM/director/bin/twgstart`

You also can use the standard RPM commands.

Uninstalling an IBM Director feature

Complete the following steps to remove a feature:

1. Modify the diruninstall script, which is located in the IBM/director/bin directory. (By default, this script removes all detected IBM Director components.)
2. Stop IBM Director Agent. Type the following command and press Enter:

   ```
   /opt/IBM/director/bin/twgstop
   ```
3. Run the diruninstall script.
4. Start IBM Director Agent. Type the following command and press Enter:

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

You also can use the standard RPM commands.

Uninstalling IBM Director

You can use the following procedures to uninstall IBM Director.

Uninstalling IBM Director on Windows

Complete the following steps to uninstall IBM Director:

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 you want to remove; then, click **Remove**.
4. Follow the instructions on the screen.

Uninstalling IBM Director Agent on Linux

Use the diruninstall script located in the IBM/director/bin director. Running this script will remove all IBM Director components. To uninstall IBM Director Agent, type the following command and press Enter:

```
/opt/IBM/director/bin/diruninstall
```

You also can use standard RPM commands.

Chapter 9. IBM Director Agent — IBM Director Server security

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.

How it works

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 allows holders 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.

Managed systems running Linux are secured by default. You can secure managed systems running Windows manually or during discovery.

Note: The IBM Director Agent running on a management server is automatically secured. It will have a trust relationship only with the IBM Director Server installed on the same system.

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.

Once the managed system has been secured by a management server, only that management server (and other management servers that had previously established a trust relationship) 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 dsa*xxxxx*.pub files, where *xxxxx* is a unique identifier. The private keys held by IBM Director Server are stored in dsa*xxxxx*.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 what options were selected during the installation of IBM Director Agent.

By default, the files are located in the following directories.

Operating system	Directory
Windows 2000	*c*:\Program Files\IBM\Director\Data
Linux	/opt/IBM/director/data

where *c* is 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 what operating system it is running. Managed systems running Linux are set to the secure state by default.

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 decides to secure 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 will no longer

accept any new public keys from management servers. However, the managed system will continue 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 automatically secure unsecured managed systems, 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. You can use this procedure to secure either an unsecured or a secured system:

1. If you have not done so already, install and start IBM Director Server. IBM Director Server will create 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-line prompt, type the following command and press Enter:

   ```
   net stop twgipc
   ```
4. Delete all existing dsa*.pub files from the managed system. If IBM Director Agent is installed in the default location, the files are located in the *c*:\Program Files\IBM\director\data directory, where *c* is the hard disk where IBM Director Agent is installed.
5. Place the dsa*.pub and secin.ini files (that you copied in step 2) into the following directory: *c*:\Program Files\IBM\director\data, where *c* is the hard disk where IBM Director Agent is installed, and IBM Director Agent is installed in the default directory.
6. Restart IBM Director Agent. From a command-line prompt, type the following command and press Enter:

   ```
   net start twgipc
   ```

After IBM Director Agent starts, the managed system is secure; it will permit *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 will appear in the Group Contents pane of IBM Director Console with a padlock icon next to 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 52. 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 can also copy the dsa*.pub file from the management server to the managed system. After the managed system is restarted, it will trust the new management server.

Removing access to a managed system

To revoke a management server access to 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 DSA*xxxx*, 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. Stop IBM Director Agent. From the command prompt, type one of the following commands and press Enter:

Windows 2000	`net stop twgipc`
Linux	`/opt/IBM/director/twgstop`

5. Restart IBM Director Agent. Type one of the following commands and press Enter:

Windows 2000	`net start twgipc`
Linux	`/opt/IBM/director/twgstart`

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:

- Setup 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 begins delivering 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.
- Setup the new server, install IBM Director Server, and copy the dsa*.pvt file from an existing trusted management server. This allows the new management server to immediately authenticate itself to the managed systems that trusted the existing management server. The new management server also will be 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 which 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:

*XXXX*DSA*KeytypeString*

where:

- *XXXX* is a four-character header.
- *String* is the name of the management server that generated the key file.
- *Keytype* indicates the type of the key. “P” denotes public, and “p” denotes private.

For example, “DSAPdirector4_1” indicates a public key file generated by a management server named director4_1, and “DSApdirector4_1” indicates the private 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 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 73.

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.

Chapter 10. Solving IBM Director problems

The following table lists some of the problem symptoms and suggested solutions for IBM Director 4.0.

Symptom	Suggested action
Databases	
The Microsoft Jet database is full.	Migrate to a larger database such as IBM DB2®, Oracle, or Microsoft SQL.
Errors appear during the Database Configuration process when an Oracle database is used.	Configure and start the Oracle TCP/IP listener before starting the Database Configuration dialog. If a failure occurs, the database administrator must check the configuration of the TCP/IP listener.
Dialog boxes	
Tables appear too small in a pane.	Change the table settings to enlarge the table in the pane. **Note:** Modified table settings are not saved.
Dynamic groups criteria	

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 do not possess that criterion are returned.	Verify that you are using the correct criteria when you create the dynamic group. Each criterion searches only the rows in the table with which it is associated. For example:
	• If you select a criterion of
	`Inventory (PC)/SCSI Device/Device Type=TAPE`
	only the managed systems that appear in at least one row in the SCSI_DEVICE table that also have a value of TAPE in the DEVICE_TYPE column are returned.
	• If you select a criterion of
	`Inventory (PC) / SCSI Device/Device Type ^= TAPE`
	only the managed systems that appear in at least one row of the SCSI_DEVICE table, of which none of those rows have a value of TAPE in the DEVICE_TYPE column, are returned. This does not necessarily return all managed systems that do not have SCSI tape drives. Only managed systems that appear in a particular table and that meet the criteria for that table are returned.

Event action plans	
Group event action plans do not appear.	Verify that a managed system or group has an event action plan assigned to it: 1. In IBM Director Console, click **Associations** → **Event Action Plans**. 2. In the Groups pane, click **All Groups**. 3. In the Group Category Contents pane, expand each group that has an event action plan applied to it to view the event action plans that are applied to the group. Event action plan associations are not displayed in the Groups pane, nor are event action plans that have been applied to a group displayed as being associated with each individual managed system that is a part of that group. The event action plan is displayed as being applied to the group only.

Symptom	Suggested action
Event log message	
An event ID 2003 warning message appears in the application event log.	If you are using Windows 2000 with Internet Information Services (IIS) installed, an event ID 2003 warning message might appear in the application event log when you start System Monitor and add counters. The event ID 2003 warning message might appear as follows: `The configuration information of the performance library "C:\WINNT\system32\w3ctrs.dll" for the "W3SVC" service does not match the trusted performance library information stored in the registry.` The functions in this library are not recognized as trusted. Microsoft previously identified that this is a problem in these products.
Field replaceable unit (FRU)	

FRU information does not appear when inventory is collected.	Verify that the FTP client (director\cimom\bin\getfru.exe) is able to reach the IBM FRU information site through your firewall. For the copy to succeed, the managed system must have firewall access through a standard FTP port. By default, it tries to reach ftp://ftp.pc.ibm.com/pub/pccbbs/bp_server on port 21. If the managed system cannot access the IBM Support FTP site, you can copy the FRU files to your network manually. Use the program getfru.exe which is in the %SystemRoot%\system32 directory. Type the following command from a command prompt:
	`getfru -s ftp.pc.ibm.com -d /pub/pccbbs/bp_server`
	
	Copy the FRU data files to a server and directory on your network. Then, write a script to retrieve these files automatically. To use the getfru.exe program in your script, observe the following syntax:
	`getfru -s <ftp_server_name> -d <directory_of_fru_files>`
	
	where:
	• *ftp_server_name* is the FTP address of the network server where you copied the FRU data files.
	• *directory_of_fru_files* is the directory that stores the FRU data files.
	
	Then, use the Process Management task to run the FRU data files located on your network. See *IBM Director 4.0 for BladeCenter products Systems Management Guide* for more information. If the FRU Numbers service does not detect the presence of the FRU data files, some FRU information might be available from other sources for the FRU Numbers service to display.

Hard disk drives geometry reporting	
The following report is created indicating that an insufficient amount of space is available on a hard disk drive: `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 a Microsoft operating system: • Optical • Iomega • Jaz This is previously identified by Microsoft as a Windows Management Instrumentation (WMI) problem.

Symptom	Suggested action
IBM Director Console	
Managed systems are unavailable on the management console.	• Verify that: – The system is turned on. – IBM Director Agent is running. – The network connection is reliable. • Check or modify the network timeout value. Click **Start** → **Programs** → **IBM Director** → **Network Configuration**. • Check the network timeout value for the management server or the managed system. To change the network timeout value using: – **Windows**: Open the twgipccf.exe file, and change the timeout value. – **Linux**: In the data directory, under the products install root, edit the ServiceNodeLocal.properties file. Add `ipc.timeouts=x` where *x* is the specified number of seconds. The default setting is 15 seconds. If you are using UNIX or Linux and IBM Director Agent is installed in the default directory, you must restart the managed system. From a command prompt, type `/opt/IBM/director/bin/twgend -r` to stop and restart the managed system.
An input/output error connecting-to-server message appears when IBM Director Console is started.	Make sure that IBM Director Server is running before starting IBM Director Console. A green circle icon in the task bar is displayed to indicate that you can start IBM Director Console. Do not attempt to start IBM Director Console if the red diamond icon (indicating that the server is not responding) or the green triangle icon (indicating that the server is still in the process of starting) appear in the task bar.
Errors appear during attempts to log on to the management server using IBM Director Console.	Verify that: • The management server name, user ID, and password are valid. • The management server is running.
A request for access fails, and the managed systems remain locked.	• Determine whether the managed system and management server accept encrypted communications only. • Ensure that the server has encryption enabled through the Encryption Administration window. • If the managed system has a UNIX or Linux operating system, ensure that the password encryption method is set to Message Digest 5 (MD5). • Make sure that you have a connection from the management console to port 2033 on the management server.
Through the use of imaging, a system was added and appears on the management console as a duplicate of a system that was previously added.	Verify that the Unique ID attribute is enabled through the operating system.

Symptom	Suggested action
IBM Director Server	
IBM Director Server is not starting.	• Determine whether a service is failing that might prevent IBM Director Server from starting. Double-click the IBM Director icon on the task bar to determine whether there are any failing services. • Verify that the IBM Director Server service ID password and user account are valid. You must always use the same administrator password and user account for IBM Director Server and IBM Director Server service. To change the user account or password for the service, complete the following steps: 1. Click **Start** → **Programs** → **Administrative Tools**. 2. Double-click **Services**. 3. Right-click **IBM Director Server**. 4. Select **Properties**. Click **Log On**. 5. Select the **This account** check box, and modify and confirm the password. 6. Click **OK**, and then restart the IBM Director Server service.
Java® Runtime Environment (JRE) exceptions	
Intermittent JRE exceptions occur.	Verify that you have sufficient system memory. Intermittent JRE exceptions might occur when you run IBM Director Console on systems that are memory constrained. Sun Microsystems previously identified that this is a problem in some products. For more information about memory requirements, see Chapter 2, “Requirements for installing IBM Director” on page 5.
SNMP browser	
Opening the SNMP browser for a device does not display the specific requested MIB.	Verify that: • IBM Director is using a community name that allows read access to the MIB that you want to view. With certain SNMP devices you can hide MIBs behind community names. • The SNMP device or agent implements the MIB in question.
SNMP devices	
SNMP devices are not being discovered.	Verify that: • The management server is running the SNMP service. If it is not, another system on the same subnet must be running an SNMP agent and must be added as a seed device. Remove the management server as the seed device. • The seed devices or other devices to be discovered are running an SNMP agent. • The community names specified in the IBM Director Discovery Preferences window allow IBM Director to read the mib-2.system table of the devices to be discovered and the mib-2.at table on seed devices. • The correct network masks have been configured for all managed systems that must be discovered. • The 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 **Options** → **Discovery Preferences**. SNMP discovery does not discover 100% of the devices. If a device has not communicated with other managed systems, the device might not be discovered.

Symptom	Suggested action
An attribute value for a MIB file cannot be changed.	Verify that: • IBM Director is using a community name that allows write access to the MIB file that has a value that you want to change. • The MIB file is writable. • The MIB file has a value you can set to be displayed in the SNMP browser. • The compiled MIB file is associated with the value to change.
When a MIB file attribute value is set to a hexadecimal, octal, or binary value, the file fails.	Verify that all values have been converted and are being added in a decimal format.
SNMP traps	
Trap destinations are missing from the SNMP agent table. **Note:** IBM Director sends and receives SNMP traps using TCP/IP only.	A table displays only the first trap destination in the SNMP configuration interface when there are multiple communities and traps associated with each community. The IBM Director CIM-based inventory stores only the first value of an array-valued property (such as the SNMP trap destination).
Security	
Load All Events does not function.	When the security log gets very large (approximately 4000 records), clicking **Load All Events** produces the `Loading data...please wait` message. After approximately 5 minutes, the message stops, and only the 30 most recent events are displayed. The **Load All Events** button is not enabled.
Software Distribution	
The software distribution package creation fails.	Check the available disk space on the management server. Packages are created on the management server before being written to the target system. If disk space is insufficient on the management server, the package creation fails.
An error message appears when a software package is distributed using a redirector share.	The error message is: `Managed System (system name) has detected that software package (package name) was not found on share (\\server\share).` You can delete software-distribution packages from the management server. The redirector cache can be maintained only through the File Distribution Server Managers interface. This is accessed by right-clicking the **Software Distribution** task. Errors occur if you manipulate the cache through any means other than IBM Director Console.
Software-distribution packages are not using the file-distribution servers.	Ensure that the file-distribution server is a member of the same domain as the management server or has a trust relationship with that domain.
The software-distribution package installation failed, and the location of the package needs to be changed.	Reinstall IBM Director Agent, and specify a different drive and directory.
Redirected software distributions are not working properly.	If Norton AntiVirus is installed on the management server, redirected distributions fail. Complete the following steps: 1. Uninstall Norton AntiVirus. 2. Delete the failed software distribution packages. 3. Recreate the packages.
Time zone	
The wrong time zone is displayed.	When the time zone is changed, a managed system does not adjust the time shown in the event viewer. Start the managed system again to show the correct time for the new time zone.

Appendix A. Terminology summary and abbreviation list

This appendix provides a summary of IBM Director terminology and a list of abbreviations used in IBM Director publications.

IBM Director terminology summary

The following terminology is used in the IBM Director publications.

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.

The *IBM Director service account* is an operating-system user account on the management server. This account is used to install IBM Director Server and is the account under which the IBM Director Service runs.

The *database server* is the server on which the database application is installed.

Abbreviation	Definition
ASF	Alert Standard Format
ASM	Advanced System Management
ASM PCI Adapter	Advanced System Management PCI adapter
BIOS	basic input/output system
CIM	Common Information Model
CIMOM	CIM Object Manager
CRC	cyclic redundancy check
CSV	comma-separated value
DBCS	double-byte character set
DES	data encryption standard
DIMM	dual inline memory module
DMI	Desktop Management Interface
DNS	Domain Name System
EEPROM	electrically erasable programmable read-only memory
FRU	field replaceable unit
FTMI	fault tolerant management interface

Abbreviation	Definition
GB	gigabyte
Gb	gigabit
GUI	graphical user interface
GUID	globally unique identifier
IIS	Microsoft Internet Information Server
I/O	input/output
IP	Internet protocol
IPC	interprocess communication
IPX	internetwork packet exchange
ISMP	integrated system management processor
JVM	Java Virtual Machine
JCE	Java Cryptography Extension
JDBC	Java Database Connectivity
JFC	Java Foundation Classes
JRE	Java Runtime Environment
KB	kilobyte
Kb	kilobit
LAN	local area network
LED	light-emitting diode
MAC	media access control
MB	megabyte
Mb	megabit
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
MSCS	Microsoft Cluster Server
NIC	network interface card
NNTP	Network News Transfer Protocol
NVRAM	nonvolatile random access memory
PCI	peripheral component interconnect
PCI-X	peripheral component interconnect-extended
PDF	Portable Document Format
PFA	Predictive Failure Analysis
RAM	random access memory
RDM	Remote Deployment Manager
RPM	Red Hat Package Manager
SID	Security identifier

Abbreviation	Definition
SMBIOS	System Management BIOS
SMS	Systems Management Server
SMTP	Simple Mail Transfer Protocol
SMART	Self-Monitoring, Analysis, and Reporting Technology
SNMP	Simple Network Management Protocol
SNA	Systems Network Architecture
SQL	Structured Query Language
SSL	Secure Sockets Layer
TAP	Telocator Alphanumeric Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TTL	time to live
UDP	User Datagram Protocol
UIM	Upward Integration Module
UNC	universal naming convention
UUID	universal unique identifier
VPD	vital product data
VRM	voltage regulator module
WfM	Wired for Management
WINS	Windows Internet Naming Service
WMI	Windows Management Instrumentation

Appendix B. 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:

- Use the troubleshooting information in your system and software documentation, and use the diagnostic tools that come with your system.
- 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.
- Use an IBM discussion forum on the IBM Web site to ask questions.

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.ibmlink.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/. If you click **Profile** from the support page, you can create a customized support page. The support page has many sources of information and ways for you to solve problems, including:

- Diagnosing problems, using the IBM Online Assistant
- Downloading the latest device drivers and updates for your products
- Viewing Frequently Asked Questions (FAQ)
- Viewing hints and tips to help you solve problems
- Participating in IBM discussion forums
- Setting up e-mail notification of technical updates about your products

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.

Appendix C. Notices

This publication 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 jurisdictions 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 publication 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.

Some software may differ from its retail version (if available) and may not include all user manuals or all program functionality.

IBM makes no representations or warranties regarding third-party products or services.

Edition notice

Note to U.S. Government Users — Documentation related to restricted rights — Use, duplication or disclosure is subject to restrictions set forth in 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:

BladeCenter	Predictive Failure Analysis
DB2	Redbooks
e-business logo	ServeRAID
IBM	TotalStorage
IntelliStation	Update*Xpress*
Light Path Diagnostics	Wake on LAN
Netfinity	xSeries
NetView	

Lotus and Domino are trademarks of Lotus Development Corporation and/or IBM 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 registered trademark of Linus Torvalds.

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

Index

E

F

H

I

J

K

L

M

N

Part Number: 01R0513

Printed in U.S.A.

(1P) P/N: 01R0513

SC01-R051-30