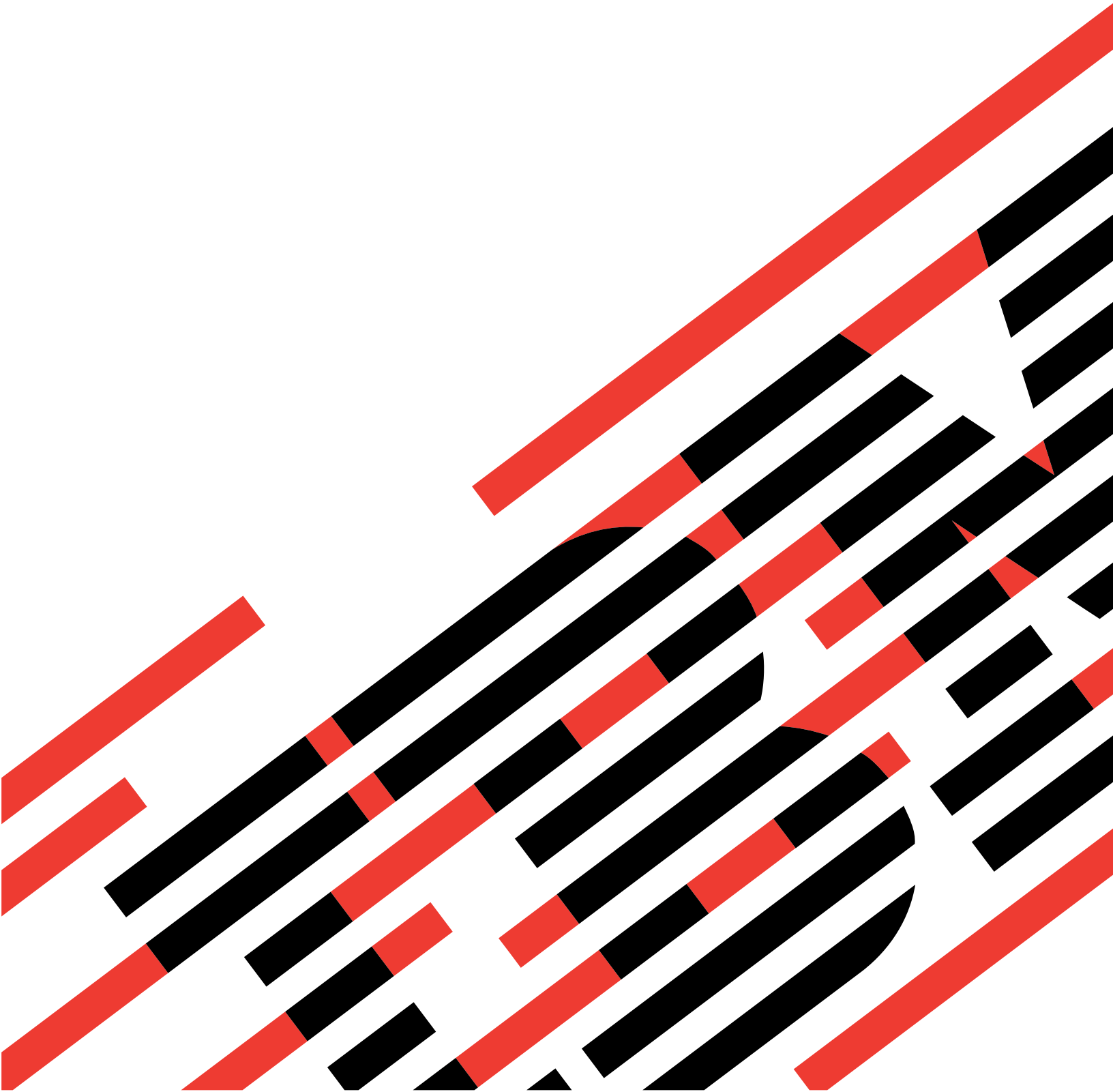
IBM

eserver

BladeCenter Management Module
User's Guide



IBM

@server

BladeCenter Management Module
User's Guide

Note: Before using this information and the product it supports, read the general information in Appendix B, “Notices,” on page 59.

Fourth Edition (February 2004)

Contents

Safety

Before installing this product, read the Safety Information.

قبل تركيب هذا المنتج، يجب قراءة الملاحظات الآمنية

Antes de instalar este produto, leia as Informações de Segurança.

在安装本产品之前，请仔细阅读 Safety Information
(安全信息)。

安裝本產品之前，請先閱讀「安全資訊」。

Prije instalacije ovog produkta obavezno pročitajte Sigurnosne Upute.

Před instalací tohoto produktu si přečtěte příručku bezpečnostních instrukcí.

Læs sikkerhedsforskrifterne, før du installerer dette produkt.

Lees voordat u dit product installeert eerst de veiligheidsvoorschriften.

Ennen kuin asennat tämän tuotteen, lue turvaohjeet kohdasta Safety Information.

Avant d'installer ce produit, lisez les consignes de sécurité.

Vor der Installation dieses Produkts die Sicherheitshinweise lesen.

Πριν εγκαταστήσετε το προϊόν αυτό, διαβάστε τις πληροφορίες ασφάλειας
(safety information).

לפני שתתקינו מוצר זה, קראו את הוראות הבטיחות.

A termék telepítése előtt olvassa el a Biztonsági előírásokat!

Prima di installare questo prodotto, leggere le Informazioni sulla Sicurezza.

製品の設置の前に、安全情報をお読みください。

본 제품을 설치하기 전에 안전 정보를 읽으십시오.

Пред да се инсталира овој продукт, прочитајте информацијата за безбедност.

Les sikkerhetsinformasjonen (Safety Information) før du installerer dette produktet.

Przed zainstalowaniem tego produktu, należy zapoznać się
z książką "Informacje dotyczące bezpieczeństwa" (Safety Information).

Antes de instalar este produto, leia as Informações sobre Segurança.

Перед установкой продукта прочтите инструкции по
технике безопасности.

Pred inštaláciou tohto zariadenia si pečítaje Bezpečnostné predpisy.

Pred namestitvijo tega proizvoda preberite Varnostne informacije.

Antes de instalar este producto, lea la información de seguridad.

Läs säkerhetsinformationen innan du installerar den här produkten.

Statement 1:

DANGER

Electrical current from power, telephone, and communication cables is hazardous.

To avoid a shock hazard:

- **Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.**
- **Connect all power cords to a properly wired and grounded electrical outlet.**
- **Connect to properly wired outlets any equipment that will be attached to this product.**
- **When possible, use one hand only to connect or disconnect signal cables.**
- **Never turn on any equipment when there is evidence of fire, water, or structural damage.**
- **Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.**
- **Connect and disconnect cables as described in the following table when installing, moving, or opening covers on this product or attached devices.**

To Connect:	**To Disconnect:**
1. Turn everything OFF.	1. Turn everything OFF.
2. First, attach all cables to devices.	2. First, remove power cords from outlet.
3. Attach signal cables to connectors.	3. Remove signal cables from connectors.
4. Attach power cords to outlet.	4. Remove all cables from devices.
5. Turn device ON.	

Statement 8:

CAUTION:
Never remove the cover on a power supply or any part that has the following label attached.

Hazardous voltage, current, and energy levels are present inside any component that has this label attached. There are no serviceable parts inside these components. If you suspect a problem with one of these parts, contact a service technician.

WARNING: Handling the cord on this product or cords associated with accessories sold with this product, will expose you to lead, a chemical known to the State of California to cause cancer, and birth defects or other reproductive harm. ***Wash hands after handling.***

ADVERTENCIA: El contacto con el cable de este producto o con cables de accesorios que se venden junto con este producto, pueden exponerle al plomo, un elemento químico que en el estado de California de los Estados Unidos está considerado como un causante de cancer y de defectos congénitos, además de otros riesgos reproductivos. ***Lávese las manos después de usar el producto.***

Chapter 1. Introducing the BladeCenter management module

This *Management Module User's Guide* contains information about configuring the management module and managing components installed in the IBM® @server BladeCenter™ unit.

Your BladeCenter unit comes with one hot-swap management module in management-module bay 1. You can add an additional management module in management-module bay 2. Only one of these management modules can be active at one time, functioning as the primary management module; a second management module, if present, provides redundancy. The secondary management module remains inactive until it is switched to act as primary.

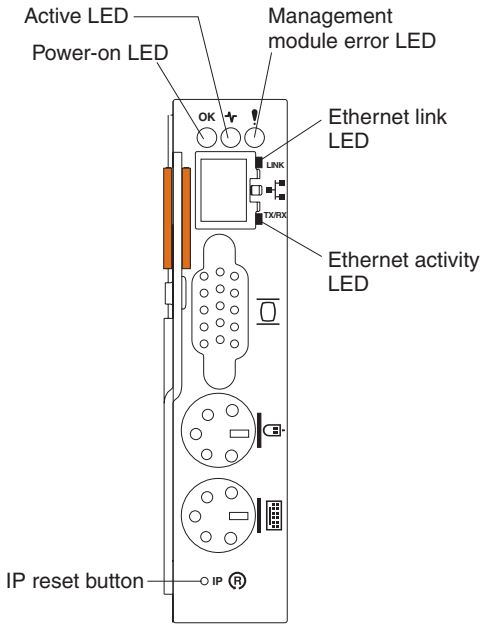
When two management modules are installed in the BladeCenter unit, both management modules must always have the same level of firmware, at a level that supports redundant management module function. This helps ensure a smooth changeover of control from the active management module to the redundant management module. The latest level of management-module firmware is available at the IBM Support Web site at http://www.ibm.com/pc/support/.

The management module functions as a service processor and a keyboard/video/mouse (KVM) multiplexor for all of the blade servers installed in the BladeCenter unit. It provides the following external connections: keyboard, mouse, and video, for use by a local console, and one RJ-45 connector for a 10/100 Mbps Ethernet remote management connection.

The service processor in the management module communicates with the service processor in each blade server to support features such as: blade server power-on requests, error and event reporting, KVM requests, and requests to use the BladeCenter shared media tray (diskette drive, CD-ROM drive, and USB port).

You configure BladeCenter components using the management module, setting information such as IP addresses. The management module communicates with all components installed in the BladeCenter unit, detecting their presence or absence, reporting their status, and sending alerts for error conditions when required.

Management module controls and indicators



Management module LEDs: These LEDs provide status information about the management module and remote management connection. For additional information, see the “Light path diagnostics” section in the *Hardware Maintenance Manual and Troubleshooting Guide* on the IBM *BladeCenter Documentation* CD.

- **Power-on:** When this green LED is lit, the management module has power.
- **Active:** When this green LED is lit, it indicates that this management module is actively controlling the BladeCenter unit.

  Note: Only one management module actively controls the BladeCenter unit. If there are two management modules installed in the BladeCenter unit, this LED is lit on only one.
- **Management module error:** When this amber LED is lit, it indicates that an error has been detected somewhere on this management module. When this indicator is lit, the system error LED on each of the BladeCenter system LED panels is also lit.
- **Ethernet link:** When this green LED is lit, there is an active connection through the port to the network.
- **Ethernet activity:** When this green LED is flashing, it indicates that there is activity through the port over the network link.

Management module IP reset button: Do not press this button unless you intend to erase your configured IP addresses for the management module and lose connection with the remote management station, the I/O modules, and the blade servers. If you press this button, you will need to reconfigure the management module settings (see the information beginning with “Setting up the remote connection” on page 7 for instructions). Use a straightened paper clip to press the recessed button in one of the following sequences to reset management-module settings:

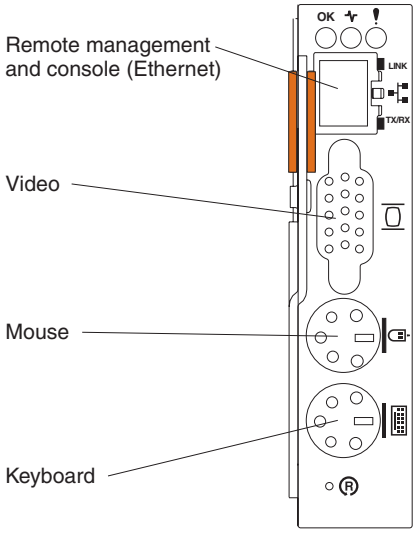
- Press the IP reset button for 3 seconds or less; then, restart the management module to reset the IP configuration of the management module network interfaces (Ethernet 1, Ethernet 2, gateway address, and so forth) to the factory defaults.

- Press the IP reset button for 5 seconds, release it for 5 seconds; then; press it again for 10 seconds and restart the management module to reset all of the management-module configuration fields to the factory defaults.

Management module input/output connectors

The management module has the following I/O connectors:
- One video
- One PS/2® keyboard
- One PS/2 mouse
- One 10/100 Mbps Ethernet for remote management and console

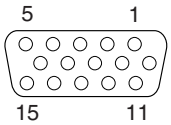
The following illustration shows the I/O connectors on the management module.



Note: There is no internal connections between the input/output connectors on the management modules when two are installed in the BladeCenter unit. See the *IBM BladeCenter Management Module Installation Guide* for information about how to cable two management modules to support the redundant management module interface requirements of your installation.

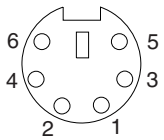
Video connector

Your BladeCenter management module contains one standard video connector. Use this connector to connect a compatible SVGA or VGA video monitor to the BladeCenter unit. Blade server integrated video controllers share the management-module video connector through the BladeCenter KVM interface.



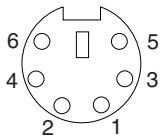
Keyboard connector

Your BladeCenter management module contains one PS/2-style keyboard connector. Use this connector to connect a PS/2 keyboard to the BladeCenter unit. Blade servers share the management-module keyboard connector through the BladeCenter KVM interface.



Mouse connector

Your BladeCenter management module contains one PS/2-style mouse connector. Use this connector to connect a PS/2 mouse to the BladeCenter unit. Blade servers share the management-module mouse connector through the BladeCenter KVM interface.

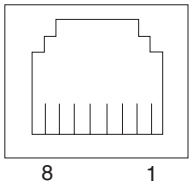


Remote management and console Ethernet connector

Your BladeCenter management module contains one 10/100 Mb Ethernet connector that provides the remote connection to the network management station on the network. Use this port to establish connections with the remote management and remote console features of the BladeCenter unit.

The network management station, through this port, can access control functions running in the service processor on each blade server or within other components installed in the BladeCenter unit. The network management station cannot use this port to communicate with application programs running in the blade servers. The network management station must direct all application related communications through a network connected to the external ports of the I/O modules installed in the BladeCenter unit, which then interface with the blade servers and their application programs.

The following illustration shows the Ethernet connector that is on the management module.



Chapter 2. Configuring the management module and BladeCenter unit

Important: You configure only the primary (active) management module. The secondary management module receives the configuration and status information automatically from the primary management module when necessary. The configuration information in this chapter applies to the primary management module, which might be the only management module installed in the BladeCenter unit.

When the BladeCenter unit is started initially, it automatically configures the remote management port on the active (primary) management module, so that you can configure and manage BladeCenter components. You configure and manage BladeCenter components remotely using the management-module Web interface or the management-module command-line interface.

Note: You can also configure the I/O modules directly through an external I/O module port, using a Telnet interface or a Web browser. See the documentation that comes with each I/O module for information.

For the management module to communicate with the I/O modules in the BladeCenter unit, you will need to configure the IP addresses for the following internal and external ports:

- The IP address for the external Ethernet (remote management) port on the management module (see the information beginning on page 30 for instructions). The initial automatic configuration of the management module enables the network management station to connect to the management module to configure the port completely and to configure the rest of the BladeCenter unit.
- The IP address for the internal Ethernet port on the management module (see the information beginning on page 30 for instructions) to support communication with the I/O modules.
- The IP address for the management port on each I/O module (see the information beginning on page 25 for instructions) for communication with the management module. You configure this port by configuring the IP address for the I/O module.

  Note: Some types of I/O modules, such as a pass-thru module, have no management port.

To communicate with the blade servers for functions such as deploying an operating system or application program, you also will need to configure at least one external (in-band) port on an Ethernet I/O module installed in I/O module bay 1 or 2. See the *Installation and User's Guide* for your BladeCenter unit for general information about configuring the external ports on Ethernet I/O modules.

Note: If a pass-thru module is installed in I/O-module bay 1 or 2 (instead of an Ethernet I/O module), you will need to configure the network switch that the pass-thru module is connected to; see the documentation that comes with the network switch for instructions.

The management module supports the following Web browsers for remote access. The Web browser that you use must be Java™-enabled, must support JavaScript™ 1.2 or later, and must have the Java 1.4.1 Plug-In installed.

- Microsoft® Internet Explorer 5.5 (with latest Service Pack installed), or later

- Netscape Navigator 4.72, or later (version 6.*x* is not supported)
- Mozilla version 1.3, or later

Notes:

1. For best results when using the Web browser, set the resolution on your monitor to 800 x 600 pixels or higher and 256 colors.
2. The Web interface does not support the double-byte character set (DBCS) languages.

The Web-based user interface communicates with the management-module Web interface and management-module command-line interface, that are part of the firmware that comes with the management module, to perform tasks such as:

- Defining the login IDs and passwords
- Selecting recipients for alert notification of specific events
- Monitoring the status of BladeCenter components
- Controlling BladeCenter components, including the blade servers
- Accessing the I/O modules to configure them
- Changing the drive startup sequence for a blade server
- Setting the date and time
- Using a remote console for the blade servers
- Changing ownership of the keyboard, video, and mouse
- Changing ownership of the CD-ROM drive, diskette drive, and USB port
- Activating On Demand blade servers

Note: The IBM Director program is a system-management product that comes with the BladeCenter unit. To configure the remote alert recipients for IBM Director over LAN, the remote alert recipient must be an IBM Director-enabled server.

You also can use the management-module Web interface and management-module command-line interface to view some of the blade server configuration settings. See Chapter 3, “Using the management-module Web interface,” on page 11 and the *IBM @server BladeCenter Management-Module Command-Line Interface Reference Guide* for more information.

Setting up the remote connection

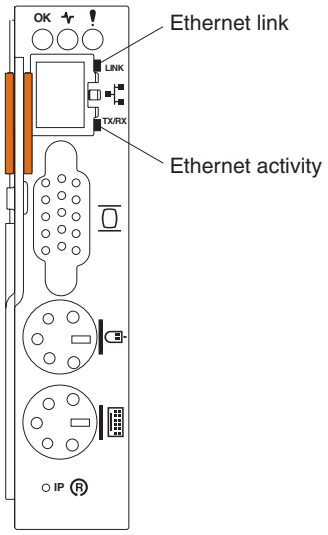
To configure and manage BladeCenter components, you must first set up the remote connection through the external Ethernet port on the management module.

Cabling the Ethernet port

Complete the following steps to connect the Ethernet cable to the management module:

1. Connect one end of a Category 5 or higher Ethernet cable to the remote management and console (Ethernet) connector on the management module. Connect the other end of the Ethernet cable to the network.
2. Check the Ethernet LEDs to ensure that the network connection is working.
   - When the green Ethernet link LED is lit, there is an active connection through the port to the network.
   - When the green Ethernet activity LED is flashing, it indicates that there is activity through the port over the network link.

   The following illustration shows the locations of the Ethernet LEDs.



Configuring the management module for remote access

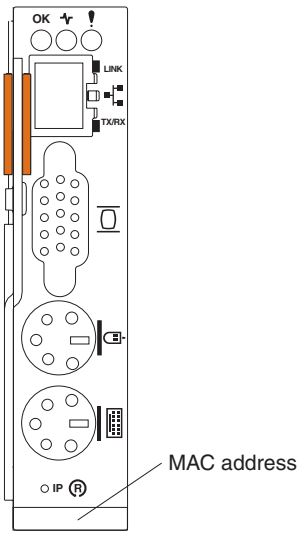
After you connect the active management module to the network, the Ethernet port connection is configured in one of the following ways:

- If you have an accessible, active, and configured dynamic host configuration protocol (DHCP) server on the network, the host name, IP address, gateway address, subnet mask, and DNS server IP address are set automatically.
- If the DHCP server does not respond within 2 minutes after the port is connected, the management module uses the factory-defined static IP address and default subnet address.

Either of these actions enables the Ethernet connection on the active management module.

Make sure your computer is on the same subnet as the management module; then, use your Web browser to connect to the management module (see “Starting the management-module Web interface” on page 12 for more information). In the browser **Address** field, specify the IP address the management module is using:

- If the IP address was assigned through a DHCP server, get the IP address from your network administrator.
- The factory-defined static IP address is 192.168.70.125, the default subnet address is 255.255.255.0, and the default host name is MM*xxxxxxxxxxxx*, where *xxxxxxxxxxxx* is the burned-in medium access control (MAC) address. The MAC address is on a label on the management module, below the IP reset button.



Note: If the IP configuration is assigned by the DHCP server, the network administrator can use the MAC address of the management module network interface to find out what IP address and host name are assigned.

Communicating with the IBM Director software

The IBM Director program is a system-management product that comes with the BladeCenter unit. The IBM Director software communicates with the BladeCenter unit through the Ethernet port on the active management module.

Note: See the IBM Support Web site at http://www.ibm.com/pc/support/ for the version of IBM Director software that you can use to manage redundant management modules.

To communicate with the BladeCenter unit, the IBM Director software needs a managed object (in the Group Contents pane of the IBM Director Management Console main window) that represents the BladeCenter unit. If the BladeCenter management module IP address is known, the network administrator can create an IBM Director managed object for the unit. If the IP address is not known, the IBM Director software can automatically discover the BladeCenter unit (out-of-band, using the Ethernet port on the BladeCenter management module) and create a managed object for the unit.

For the IBM Director software to discover the BladeCenter unit, your network must initially provide connectivity from the IBM Director server to the BladeCenter management-module Ethernet port. To establish connectivity, the management module attempts to use DHCP to acquire its initial IP address for the Ethernet port. If the DHCP request fails, the management module uses the static IP address assigned to it. Therefore, the DHCP server (if used) must be on the management LAN for your BladeCenter unit.

Notes:

1. All management modules are preconfigured with the same static IP address. You can use the management module Web interface to assign a new static IP address for each BladeCenter unit. If DHCP is not used and you do not assign a new static IP address for each BladeCenter unit before attempting to communicate with the IBM Director software, only one BladeCenter unit at a time can be added onto the network for discovery. Adding multiple units to the network without a unique IP address assignment for each BladeCenter unit results in IP address conflicts.
2. For I/O module communication with the IBM Director server through the management module external Ethernet port, the I/O module internal network interface and the management module internal and external interfaces must be on the same subnet.

Chapter 3. Using the management-module Web interface

This section provides instructions for using the management-module Web interface in the active (primary) management module. It has sections that describe:

- Features of the management-module Web interface that can be accessed by users, based on their authority level (see "User authority").
- "Starting the management-module Web interface" on page 12.
- Descriptions of the management-module Web interface screens (see "Management-module Web interface options" on page 14).
- "Network and security configuration" on page 35.
- Backup and restore of the management-module configuration (see "Using the configuration file" on page 54).

User authority

Some fields and selections in the management-module Web interface screens can only be changed or executed by users that are assigned a required level of authority for that window. Viewing information does not require any special command authority. Users with "Supervisor" command authority can change information and execute tasks in all windows.

The following table lists the management-module Web interface windows and the authority levels that are required to change information in these windows. The windows and authorities listed in this table only apply to changing the information in a window or executing a task specified in a window: viewing the information in a window does not require any special command authority. In the table, each row indicates the valid user command authorities that let a user change the information or execute a task in that window. For example, executing tasks in the **Blade Tasks → Power/Restart** window is available to users with the "Supervisor" authority or to users with the "Blade and I/O Module Power/Restart Access" authority.

Table 1. User authority relationships

Window		Authority required to change information or execute tasks								
		Supervisor	Blade Server Remote Console Access	Blade Server Remote Console and Virtual Media Access	Blade and I/O Module Power/Restart Access	Ability to Clear Event Logs	Basic Configuration (MM, I/O Modules, Blades)	Network and Security Configuration	Advanced Configuration (MM, I/O Modules, Blades)	User Account Management
Monitors	System Status	•	•	•	•	•	•	•	•	•
	Event Log (view)	•	•	•	•	•	•	•	•	•
	Event Log (clear)	•				•				
	LEDs	•	•	•	•	•	•	•	•	•
	Hardware VPD	•	•	•	•	•	•	•	•	•
	Firmware VPD	•	•	•	•	•	•	•	•	•

Table 1. User authority relationships (continued)

Window		Authority required to change information or execute tasks								
		Supervisor	Blade Server Remote Console Access	Blade Server Remote Console and Virtual Media Access	Blade and I/O Module Power/Restart Access	Ability to Clear Event Logs	Basic Configuration (MM, I/O Modules, Blades)	Network and Security Configuration	Advanced Configuration (MM, I/O Modules, Blades)	User Account Management
Blade Tasks	Power/Restart	•			•					
	On Demand	•			•					
	Remote Control (remote console)	•	•	•						
	Remote Control (virtual media)	•		•						
	Firmware Update	•							•	
	Configuration	•					•		•	
	Serial over LAN	•						•	•	
I/O Module Tasks	Power/Restart	•			•					
	Management	•						•	•	
	Firmware Update	•							•	
MM Control	General Settings	•					•		•	
	Login Profiles	•							•	•
	Alerts	•					•		•	
	Port Assignments	•						•	•	
	Network Interfaces	•						•	•	
	Network Protocols	•						•	•	
	Security	•						•	•	
	Configuration File	•							•	
	Firmware Update	•							•	
	Restore Defaults	•							•	
	Restart MM	•							•	

Starting the management-module Web interface

Complete the following steps to start the management-module Web interface program:

1. Open a Web browser. In the address or URL field, type the IP address or host name assigned for the management-module remote connection (see “Configuring the management module for remote access” on page 8 for more details).

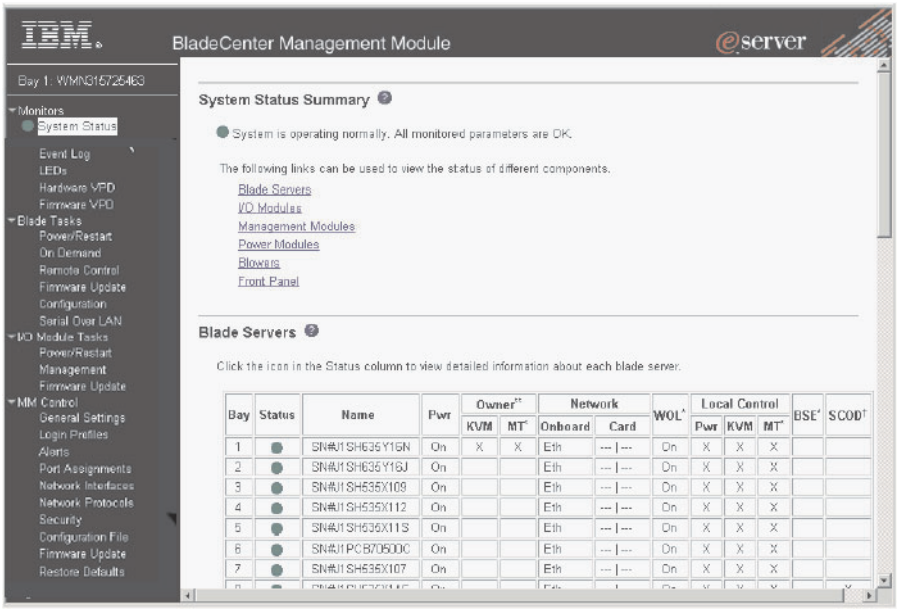
The Enter Network Password window opens.

2. Type your user name and password. If you are logging in to the management module for the first time, you can obtain your user name and password from your system administrator. All login attempts are documented in the event log.

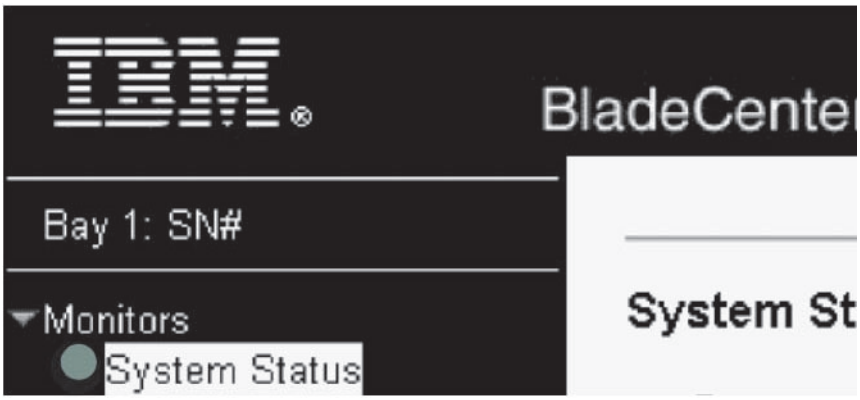
   Note: The initial factory-defined user ID and password for the management module are:
   - User ID: USERID (all capital letters)
   - Password: PASSW0RD (note the zero, not O, in PASSW0RD)

3. Follow the instructions that appear on the screen. Be sure to set the timeout value you want for your Web session.

The BladeCenter management-module Web interface window opens.



Note: The upper left corner of the management-module Web interface window shows the location and identity of the active (primary) management module. In the following example, the primary management module is identified as “SN#” and is installed in management-module bay1.



Management-module Web interface options

From the management-module Web interface is a management and configuration program that lets you select the BladeCenter settings that you want to view or change.

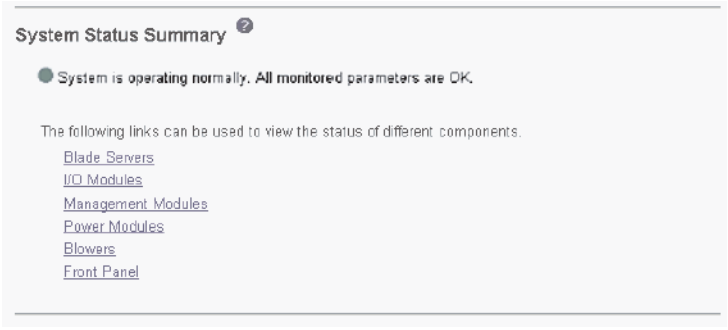
The navigation pane (on the left side of the management-module Web interface window) contains navigational links that you use to manage your BladeCenter unit and check the status of the components (modules and blade servers). Descriptions of the links that are in the navigation pane are described in the sections that follow.

Online help is provided for the management-module Web interface. Click the help (?) icon next to a section or choice to display additional information about this item.

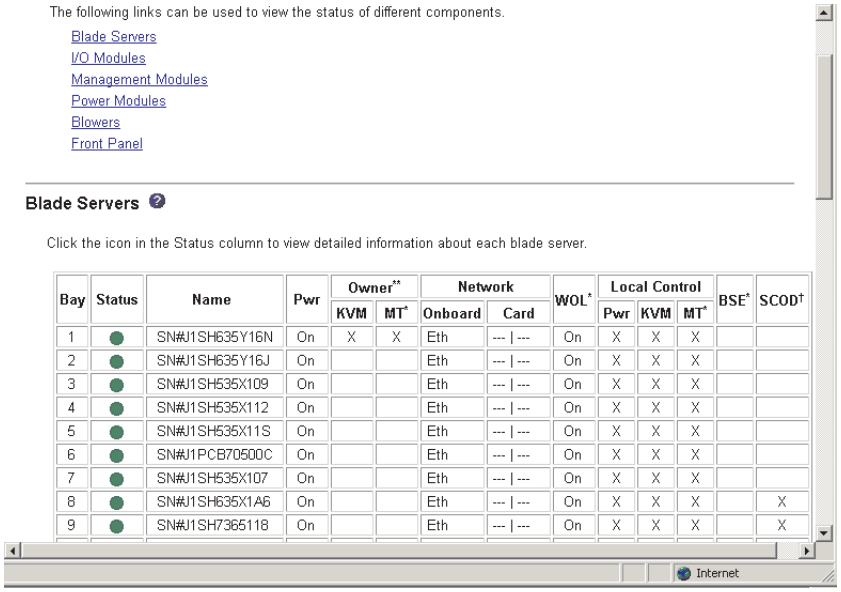
Monitors

Use the choices in the Monitors section to view the status, settings, and other information for components in the BladeCenter unit.

System Status



Select the System Status choice to view the overall system status, a list of outstanding events that require immediate attention, and the overall status of each of the blade servers and other components installed in your BladeCenter unit.



Blade Servers:

- **Bay** - The lowest-number bay the blade server occupies.

- **Status** - An icon that indicates good, warning, or bad status for the blade server. Click the icon for more detailed status information.
- **Name** - The name of the blade server.
- **Pwr** - The power state (on or off) of the blade server.
- **Owner** - An indication of whether the blade server is the current owner of the following BladeCenter resources:
  - **KVM** - Keyboard, video, and mouse.
  - **MT** - The media tray containing the CD-ROM drive, diskette drive, and USB port.
- **Network** - An indication of which network interfaces are on the blade server and the I/O expansion options. For example, an Onboard status of `eth` indicates that the blade server has integrated Ethernet controllers on the system board and a Card status of `fibre` indicates that the blade server has a Fibre Channel I/O expansion option installed.
- **WOL** - An indication of whether the Wake on LAN® feature is currently enabled for the blade server. The Wake on LAN feature is enabled by default in blade server BIOS code and cannot be disabled. The BladeCenter management module provides a single point of control for the Wake on LAN feature, enabling the settings to be controlled for either the entire BladeCenter unit or a single blade server. Wake on LAN settings made in the management module override the settings in the blade server BIOS code.
- **Local Control** - An indication of whether the following options are enabled:
  - Local power control
  - Local keyboard, video, and mouse switching
  - Local CD-ROM drive, diskette drive, and USB port switching
- **BSE** - An indication of whether a SCSI expansion unit occupies the blade bay.
- **SCOD** - An indication of whether the blade server is an On Demand blade server with a Standby status. You cannot turn on an On Demand blade server until you activate it (**Blade Tasks → On Demand**), which changes the status from Standby to Active.

  Note: You must contact IBM within 14 calendar days after you activate an On Demand blade server. See your *Agreement for Standby Capacity on Demand* for additional information.

I/O modules:

- **Bay** - The number of the bay the I/O module occupies.
- **Status** - An icon that indicates good, warning, or bad status for the I/O module.
- **Type** - The type of I/O module in the bay, such as an Ethernet I/O module, Fibre Channel I/O module, or pass-thru module.
- **MAC Address** - The medium access control (MAC) address of the I/O module.

  Note: Some types of I/O modules, such as a pass-thru module, have no MAC address nor IP address.
- **IP Address** - The IP address of the I/O module.
- **Pwr** - The power state (on or off) of the I/O module.
- **Details** - Text information about the status of the I/O module.

Management module:

- **Bay** - The number of the bay that the management module occupies.

- **Status** - An icon that indicates good, warning, or critical status for the management module. Click the icon for more detailed status information.
- **IP Address** - The IP address of the remote management and console connection (external Ethernet port) on the management module.
- **Primary** - An indication of which management module is the primary, or active, management module.

Power Modules:

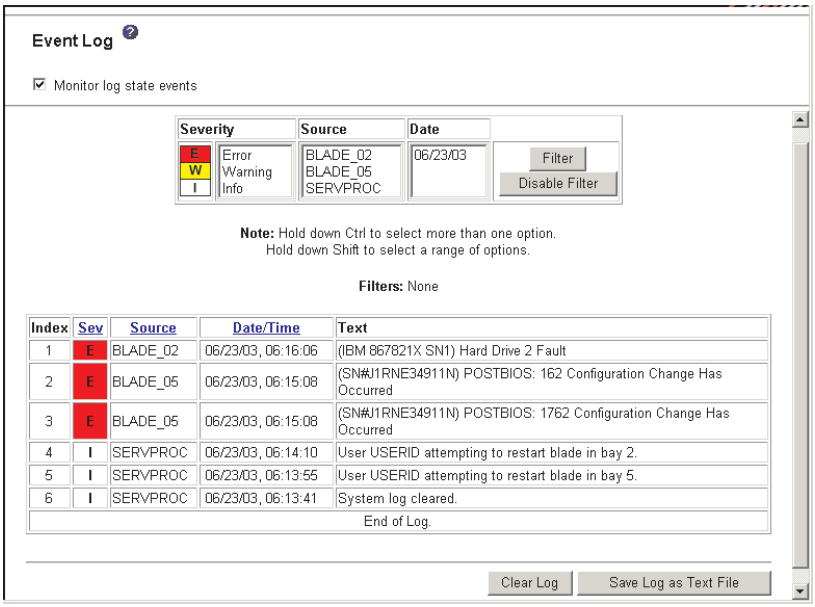
- **Bay** - The number of the bay that the power module occupies.
- **Status** - An icon that indicates good, warning, or critical status for the power module.
- **Details** - Text information about the status of the power module.

Blowers:

- **Bay** - The number of the bay that the blower module occupies.
- **Status** - An icon that indicates good, warning, or critical status for the blower module.
- **Speed** - The current speed of the blower module, as a percentage of the maximum revolutions per minute (RPMs). The blower speed varies with the thermal load. An entry of `Offline` indicates that the blower is not functioning.

Front panel: The temperature status for the front of the BladeCenter unit.

Event Log



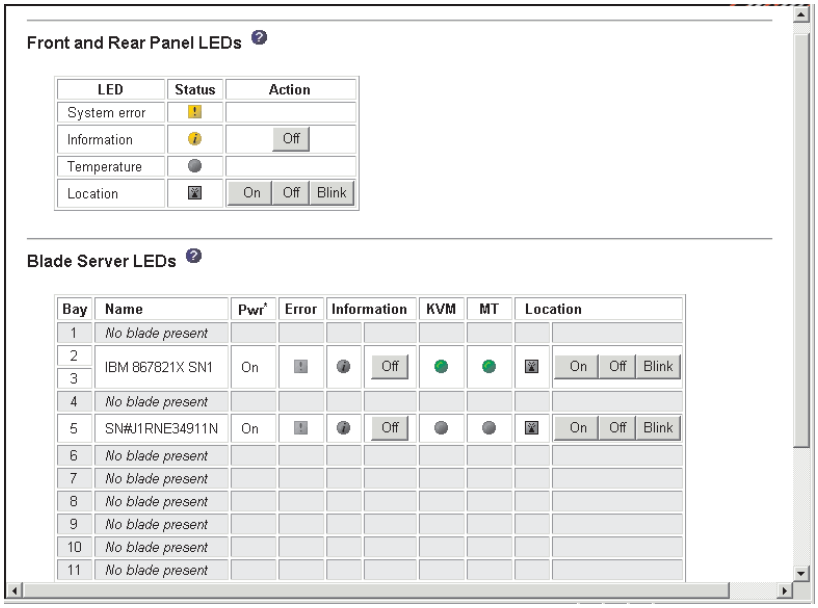
Select the Event Log choice to view entries that are currently stored in the management module event log. This log includes entries for events that are detected by the blade servers. The log displays the most recent entries first. Information about all remote access attempts is recorded in the event log, and the management module sends out the applicable alerts if configured to do so.

The maximum capacity of the event log is 750 entries. When the log is 75 percent full, the BladeCenter Information LEDs light. When the log is full, new entries overwrite the oldest entries, and the BladeCenter Error LEDs light. If you do not

want the management module to monitor the state of the event log, deselect the **Monitor log state events** checkbox at the top of the event log page.

You can sort and filter entries in the event log. See the event log help for more information.

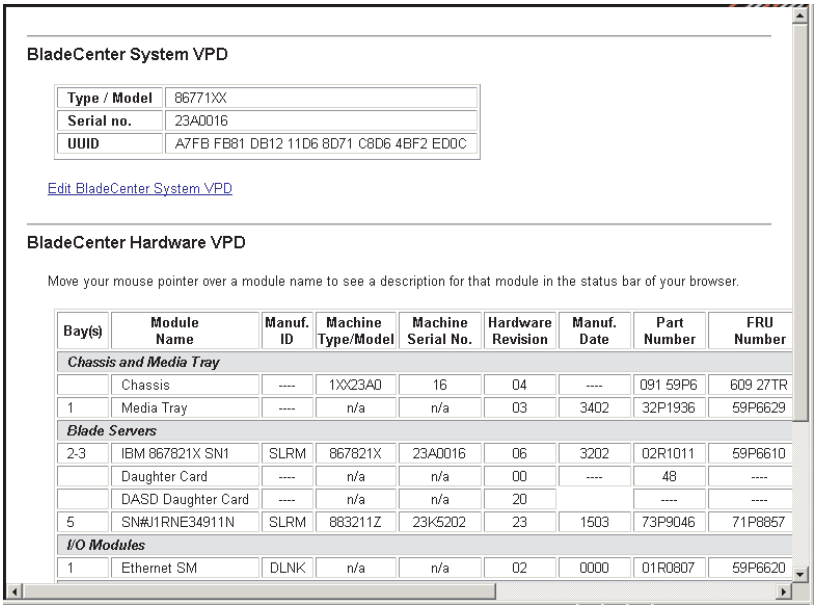
LEDs



Select the LEDs choice to view the state of the BladeCenter system LED panel and blade server control panel LEDs. You also can use this choice to turn off the information LED and turn on, turn off, or blink the location LED on the BladeCenter unit and the blade servers.

- **Front Panel LEDs** - The state of the following LEDs on the BladeCenter system LED panel. You can change the state of the information and location LEDs.
  - System error
  - Information
  - Over temperature
  - Location
- **Blade Server LEDs** - The state of the following LEDs on the blade server control panel. You can change the state of the information and location LEDs.
  - Power
  - Error
  - Information
  - Keyboard, video, and monitor select
  - Media (CD-ROM, diskette drive, USB port) select
  - Location

Hardware VPD



BladeCenter System VPD

Type / Model	86771XX
Serial no.	23A0016
UUID	A7FB FB81 DB12 11D6 8D71 C8D6 4BF2 ED0C

Edit BladeCenter System VPD

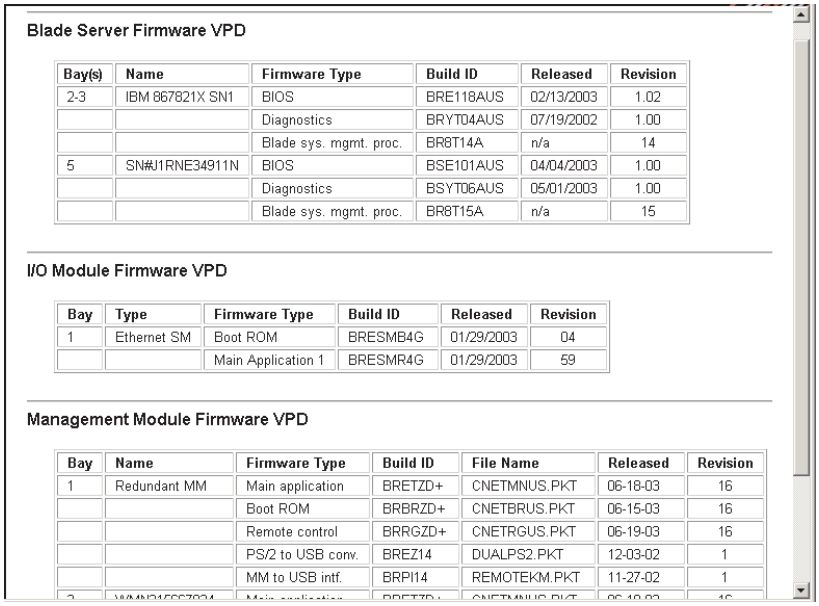
BladeCenter Hardware VPD

Move your mouse pointer over a module name to see a description for that module in the status bar of your browser.

Bay(s)	Module Name	Manuf. ID	Machine Type/Model	Machine Serial No.	Hardware Revision	Manuf. Date	Part Number	FRU Number
Chassis and Media Tray								
	Chassis	----	1XX23A0	16	04	----	091 59P6	609 27TR
1	Media Tray	----	n/a	n/a	03	3402	32P1936	59P6629
Blade Servers								
2-3	IBM 867821X SN1	SLRM	867821X	23A0016	06	3202	02R1011	59P6610
	Daughter Card	----	n/a	n/a	00	----	48	----
	DASD Daughter Card	----	n/a	n/a	20		----	----
5	SN#J1RNE34911N	SLRM	883211Z	23K5202	23	1503	73P9046	71P8857
I/O Modules								
1	Ethernet SM	DLNK	n/a	n/a	02	0000	01R0807	59P6620

Select the Hardware VPD choice to view the hardware vital product data (VPD) for the BladeCenter unit. When the BladeCenter unit is started, the management module collects the vital product data and stores it in nonvolatile memory. The management module then modifies the stored VPD as components are added to or removed from the BladeCenter unit. You can also view the log of modules inserted or removed from the BladeCenter unit.

Firmware VPD



Blade Server Firmware VPD

Bay(s)	Name	Firmware Type	Build ID	Released	Revision
2-3	IBM 867821X SN1	BIOS	BRE118AUS	02/13/2003	1.02
		Diagnostics	BRYT04AUS	07/19/2002	1.00
		Blade sys. mgmt. proc.	BR8T14A	n/a	14
5	SN#J1RNE34911N	BIOS	BSE101AUS	04/04/2003	1.00
		Diagnostics	BSYT06AUS	05/01/2003	1.00
		Blade sys. mgmt. proc.	BR8T15A	n/a	15

I/O Module Firmware VPD

Bay	Type	Firmware Type	Build ID	Released	Revision
1	Ethernet SM	Boot ROM	BRESMB4G	01/29/2003	04
		Main Application 1	BRESMR4G	01/29/2003	59

Management Module Firmware VPD

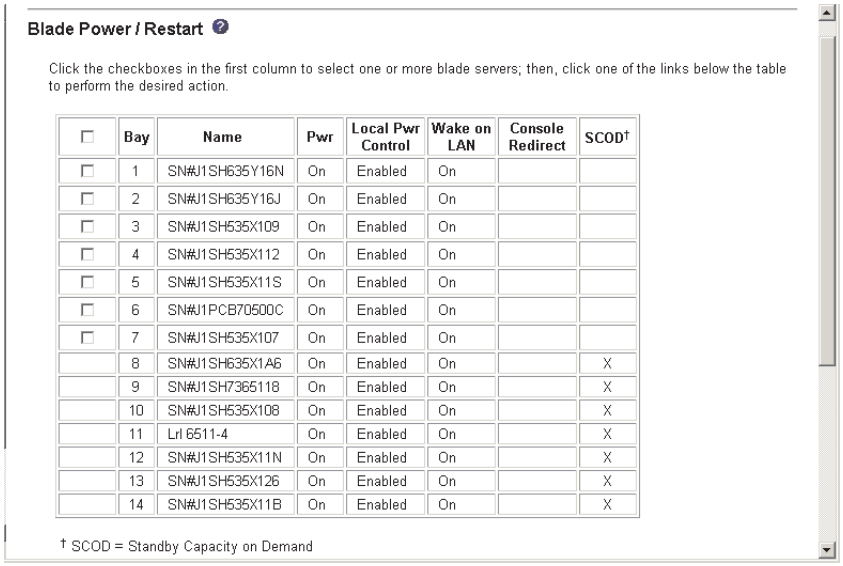
Bay	Name	Firmware Type	Build ID	File Name	Released	Revision
1	Redundant MM	Main application	BRETZD+	CNETMNUS.PKT	06-18-03	16
		Boot ROM	BRBRZD+	CNETBRUS.PKT	06-15-03	16
		Remote control	BRRGZD+	CNETRGUS.PKT	06-19-03	16
		PS/2 to USB conv.	BREZ14	DUALPS2.PKT	12-03-02	1
		MM to USB intf.	BRPI14	REMOTEKM.PKT	11-27-02	1

Select the Firmware VPD choice to view the vital product data (VPD) for the firmware in all blade servers, I/O modules, and management modules in the BladeCenter unit. The firmware VPD identifies the firmware type, build ID, release date, and revision number. The VPD for the firmware in the management modules also includes the file name of the firmware components. (Selecting the Firmware VPD choice takes up to 30 seconds to refresh and display information.)

Blade Tasks

Select the choices in the Blade Tasks section to view and change the settings or configurations of blade servers in the BladeCenter unit.

Power/Restart



Blade Power / Restart

Click the checkboxes in the first column to select one or more blade servers; then, click one of the links below the table to perform the desired action.

	Bay	Name	Pwr	Local Pwr Control	Wake on LAN	Console Redirect	SCOD†
☐	1	SN#J1SH635Y16N	On	Enabled	On		
☐	2	SN#J1SH635Y16J	On	Enabled	On		
☐	3	SN#J1SH535X109	On	Enabled	On		
☐	4	SN#J1SH535X112	On	Enabled	On		
☐	5	SN#J1SH535X11S	On	Enabled	On		
☐	6	SN#J1PCB70500C	On	Enabled	On		
☐	7	SN#J1SH535X107	On	Enabled	On		
	8	SN#J1SH635X1A6	On	Enabled	On		X
	9	SN#J1SH7365118	On	Enabled	On		X
	10	SN#J1SH535X108	On	Enabled	On		X
	11	Lrl 6511-4	On	Enabled	On		X
	12	SN#J1SH535X11N	On	Enabled	On		X
	13	SN#J1SH535X126	On	Enabled	On		X
	14	SN#J1SH535X11B	On	Enabled	On		X

† SCOD = Standby Capacity on Demand

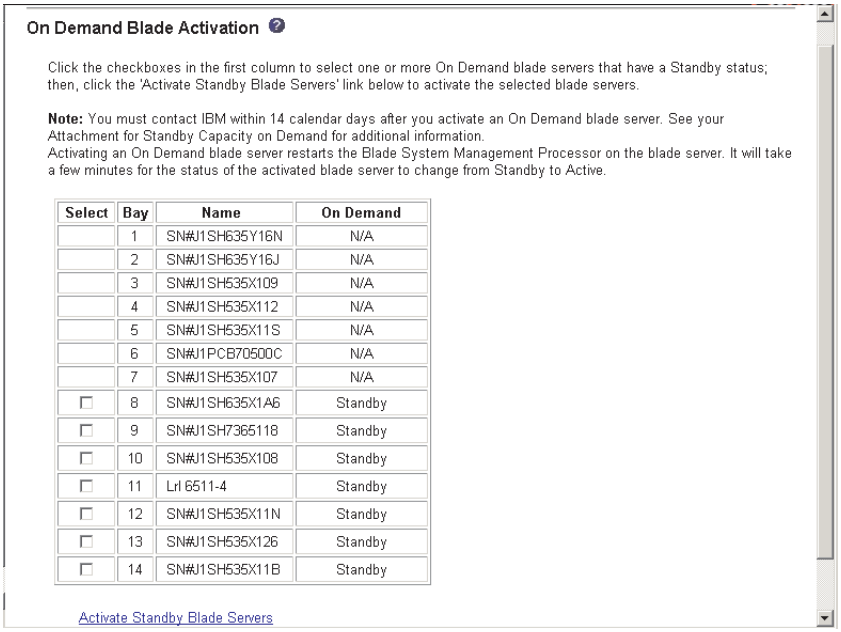
Select Power/Restart choice to perform the following actions on any blade server in the BladeCenter unit.

Note: You cannot perform these actions on an On Demand blade server with a Standby status (identified by an X in the SCOD column). To activate an On Demand blade server, see the instructions in the **On Demand** choice described in “On Demand” on page 20.

- Turn on or turn off the selected blade server (set the power state on or off).
- Enable or disable local power control. When local power control is enabled, a local user can turn on or turn off the blade server by pressing the power-control button on the blade server.
- Enable or disable the Wake on LAN feature.
- Restart the blade server or the service processor in the blade server.
- See which blade servers are currently under the control of a remote console (identified by an X in the Console Redirect column).

Select the blade servers on which you want to perform an action; then, click the appropriate link below the table for the action you want to perform.

On Demand

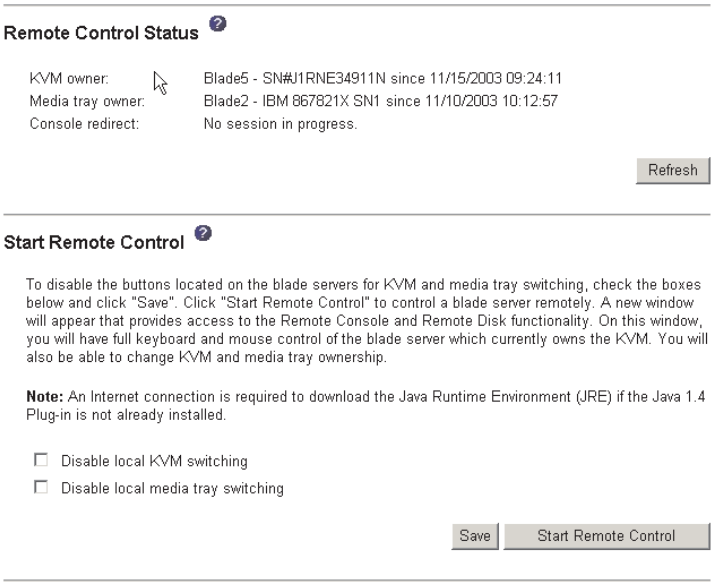


Select the On Demand choice to activate an On Demand blade server with Standby status. You must activate an On Demand blade server with Standby status before you can turn it on. When you activate an On Demand blade server, its status changes from Standby to Active, making the blade server available for use.

Select the check boxes in the Select column for one or more On Demand blade servers that have a Standby status; then, click the **Activate Standby Blade Servers** link to activate the selected blade servers. Blade servers with an On Demand status of N/A are not On Demand blade servers.

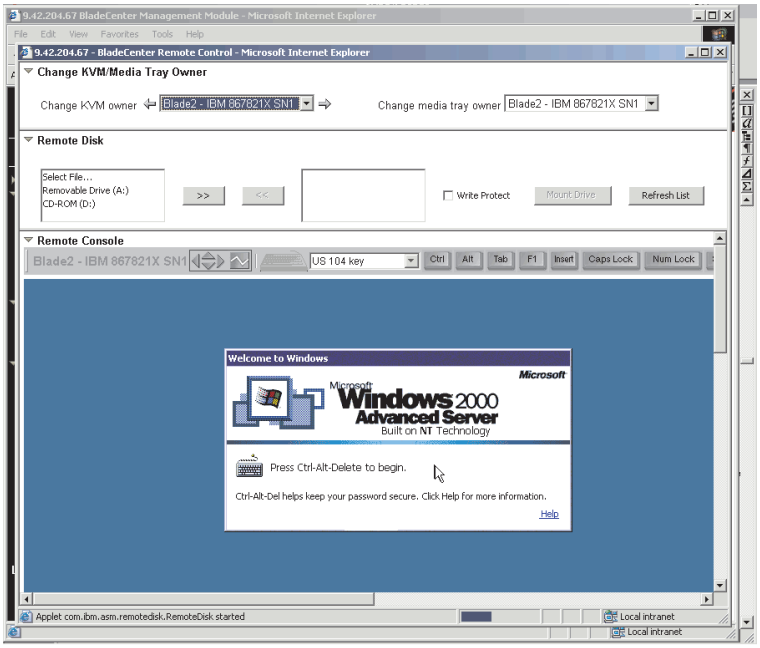
Note: You must contact IBM within 14 calendar days after you activate an On Demand blade server. See your *Agreement for Standby Capacity on Demand* for additional information.

Remote Control



Select the Remote Control choice to:

- View and change the current owners of the keyboard, monitor, and mouse (KVM), and of the CD-ROM drive, diskette drive, and USB port (Media tray).
- View the details of any remote control session currently active (user ID, client IP address, start time).
- Disable local switching of the KVM and of the media tray for all blade servers until they are explicitly enabled again. This prevents a local user from switching the console display to a different blade server while you are performing remote control tasks.
- Redirect a blade server console to the remote console.



On the remote console, you can:

- Change the owner of the KVM and of the media tray to the blade server you need to view.
- Select and access the disk drives in the media tray.
- Mount a disk drive or disk image, from the computer that is acting as the remote console, on to a blade server. The mounted disk drive or disk image will appear as a USB device attached to the blade server.
- Access files at any available network location.
- View the current blade server display.
- Control the blade server as if you were at the local console, including restarting the blade server and viewing the POST process, with full keyboard and mouse control.

Remote console keyboard support includes all keys. Icons are provided for keys that might have a special meaning to the blade server. For example, to transmit Ctrl-Alt-Del to the blade server, you must click the Ctrl icon and then press the Alt and Del keys on the keyboard.

Notes:

1. Only one remote control session is allowed at a time. If a remote control session is already active, you can end the current session and start a new one.

2. The timeout value for a remote control session is the same as the timeout value that you set for the management-module Web interface session when you logged in.
3. When you redirect a blade server Linux X Window System session console to the remote console, the ability of the remote console applet to accurately track the location of the mouse cursor depends on the configuration of the X Window system. Complete the following procedure to configure the X Window System for accurate mouse tracking. Type the commands through the remote console or at the keyboard attached to the BladeCenter unit. Note that these changes require root privileges.
   a. Enter the following commands:

      `init 3` (Switch to text mode if necessary)

      `rmmod mousedev` (Unload the mouse device driver)

   b. Add the following statement to .xinitrc in the user's home directory:

      `xset m 1 1` (Turn off mouse acceleration)

   c. Add the following statement to /etc/modules.conf:

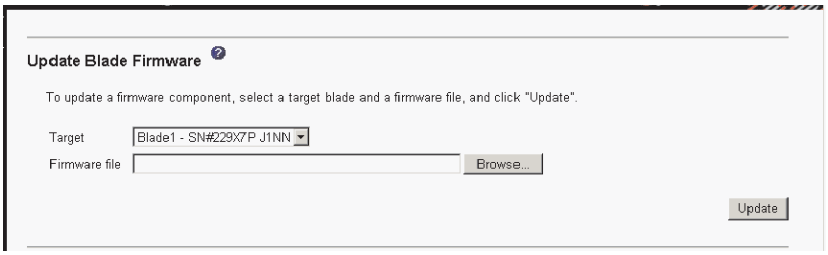
      `options mousedev xres=`*x* `yres=`*y* (Notify the mouse device driver of the video resolution) where *x* and y specify the video resolution

   d. Enter the following commands:

      `insmod mousedev` (Reload the mouse device driver)

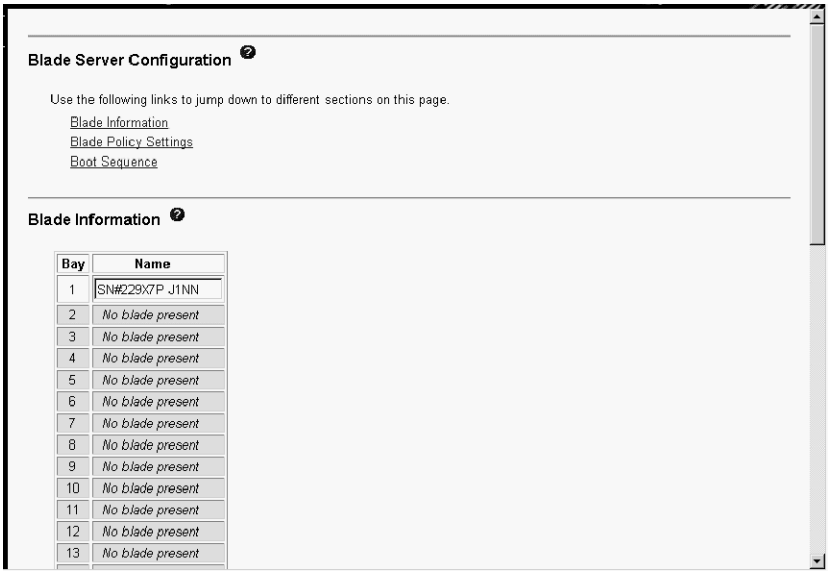
      `init 5` (Return to GUI mode if necessary)

Firmware Update



Select the Firmware Update choice to update the service processor firmware on a blade server. Select the target blade server and the firmware file to use for the update; then, click **Update**. You can obtain the firmware files from the IBM Support Web site at http://www.ibm.com/pc/support/.

Configuration

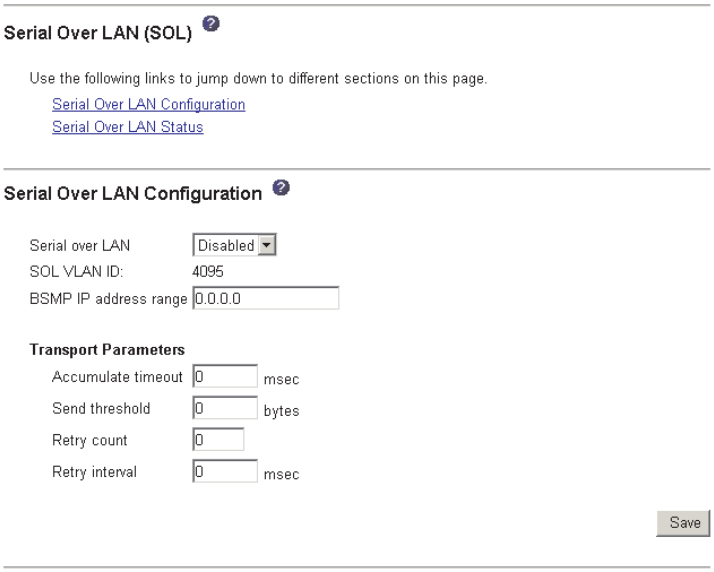


Select the Configuration choice to:

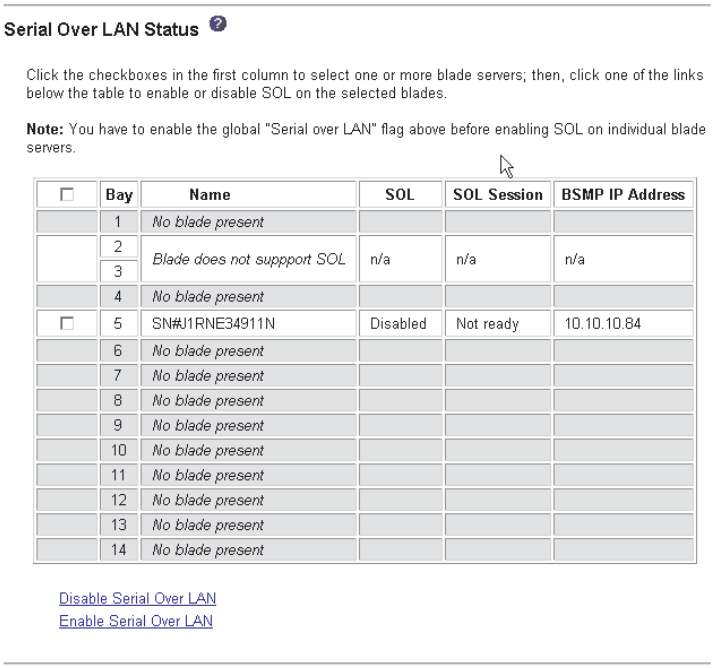
- Define a name for a blade server.
- Enable or disable the following items on all blade servers in the BladeCenter unit:
  - Local power control
  - Local KVM control
  - Local media tray control
  - The Wake on LAN feature
- View or define the startup (boot) sequence for one or more blade servers. The startup sequence prioritizes the following boot-record sources for a blade server:
  - Hard disk drives (0 through 3). The selection of hard disk drives depends on the hard disk drives that are installed in your blade server.
  - CD-ROM
  - Diskette
  - Network
    - **PXE** - Attempt a PXE/DHCP network startup the next time the selected blade server is turned on or restarted.

Note: To use the CD-ROM drive or diskette drive as a boot-record source for a blade server, the blade server must have been designated as the owner of the CD-ROM drive, diskette drive, and USB port. You set ownership either by pressing the CD/diskette/USB select button on the blade server or through the **Remote Control** choice described in “Remote Control” on page 20.

Serial Over LAN



Select the Serial Over LAN choice to view and change the global serial over LAN (SOL) settings used by all blade servers installed in the BladeCenter unit and to enable or disable SOL globally for the BladeCenter unit.



This choice also lets you monitor the SOL status for each blade server and lets you enable or disable SOL for each blade server, and globally for the BladeCenter unit. Enabling or disabling SOL globally does not effect the SOL session status for each blade server: SOL must be enabled both globally for the BladeCenter unit and individually for each blade server where you plan to start an SOL session. SOL is enabled globally and on the blade servers by default.

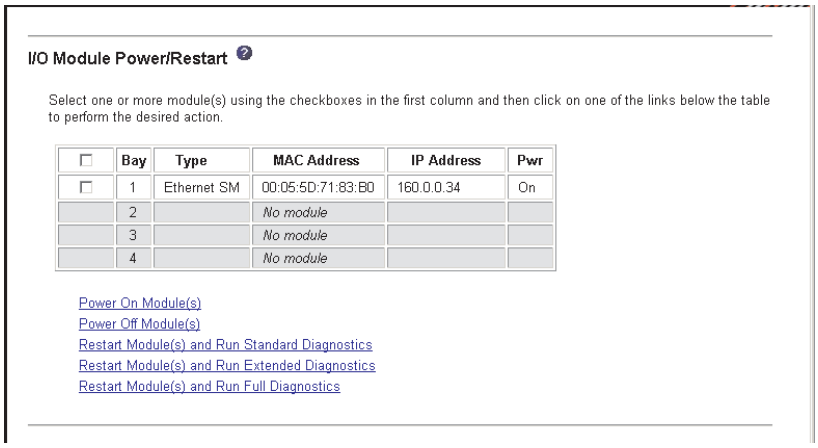
SOL sessions are started and run using the management module command-line interface. See the *IBM @server BladeCenter Management Module Command-Line Interface Reference Guide* for information and instructions.

I/O Module Tasks

Select the choices in the I/O Module Tasks section to view and change the settings or configuration on network-interface I/O modules in the BladeCenter unit.

Note: Some choices do not apply to, and are not available for, some types of I/O modules such as pass-thru modules.

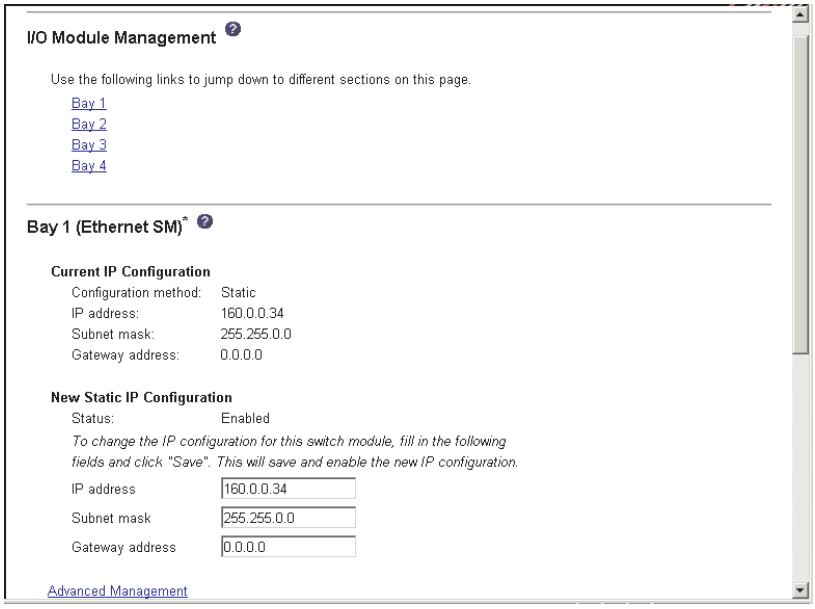
Power/Restart



Select the Power/Restart choice to display the power status of the I/O modules and perform the following actions:

- Turn on or turn off an I/O module
- Reset an I/O module

Management



Select the Management choice to view or change the IP configuration of the I/O modules; ping an I/O module; return an I/O module to the default configuration;

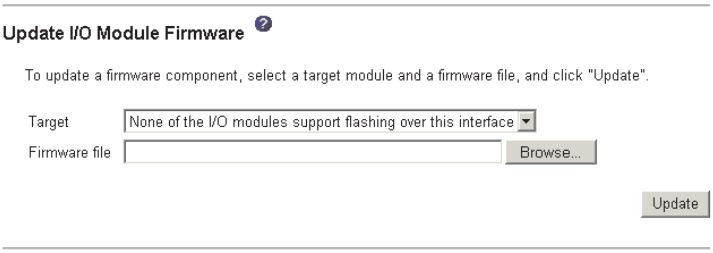
enable the I/O module ports, external management of I/O module ports, other I/O module settings; and start the configuration and management firmware that is in an I/O module.

Note: The initial factory-defined user ID and password for the I/O module firmware are:

- User ID: USERID (all capital letters)
- Password: PASSW0RD (note the zero, not O, in PASSW0RD)

See the *Installation and User's Guide* for your BladeCenter unit for more information about basic I/O module configuration. See the documentation that comes with the I/O module for details about the configuration and management firmware for the I/O module. Documentation for some I/O modules is on the IBM *BladeCenter Documentation* CD.

Firmware Update



Select the Firmware Update choice to update the firmware in a I/O module. Select the target I/O module and the firmware file to use for the update; then, click **Update**. You can obtain the firmware files from the IBM Support Web site at http://www.ibm.com/pc/support/.

MM Control

Select the choices in the MM Control section to view and change the settings or configuration on the management module that you are logged in to (the primary management module) through this management-module Web interface session. If your BladeCenter unit has redundant management modules, the configuration settings of the primary management module are automatically transferred to the secondary management module.

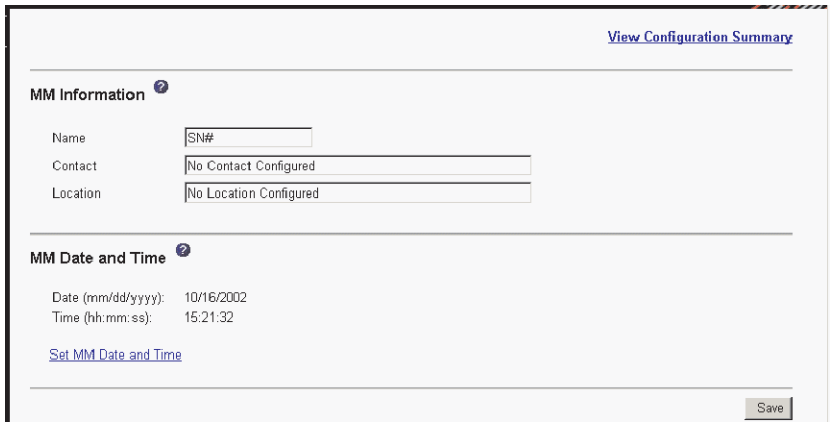
Management module configuration includes the following items:

- The name of the management module
- Up to 12 login profiles for logging in to the management module
- Ports used by the management module
- How alerts are handled
- The management module Ethernet connections for remote console and for communicating with the I/O modules
- Settings for the SNMP, DNS, SMTP, and LDAP protocols
- Settings for secure socket layer (SSL) and secure shell (SSH) security

This also includes performing the following tasks:

- Backing up and restoring the management-module configuration
- Updating the management-module firmware
- Restoring the default configuration
- Restarting the management module
- Switching from the current active management module to the redundant management module

General Settings

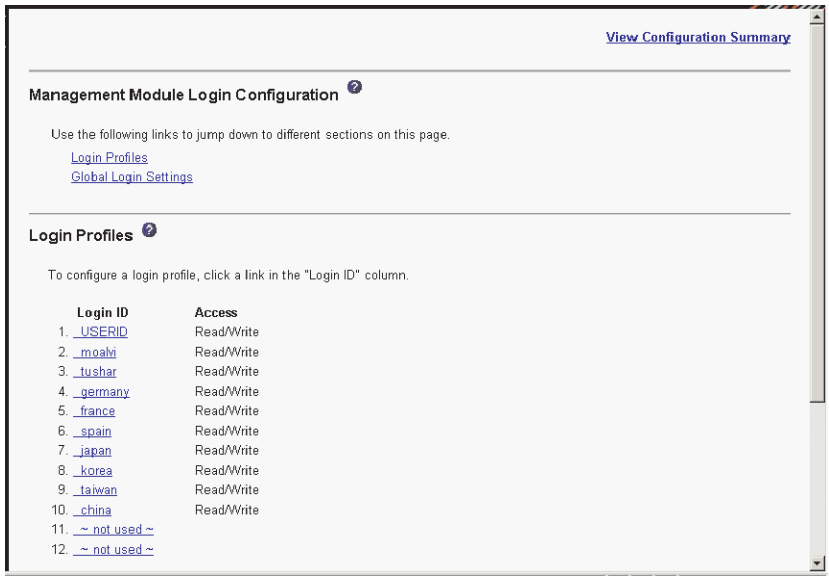


Select the General Settings choice to view or change the following settings:

- The name of the management module
- The name of the contact person responsible for the management module
- The physical location of the management module
- The real-time clock settings in the management module

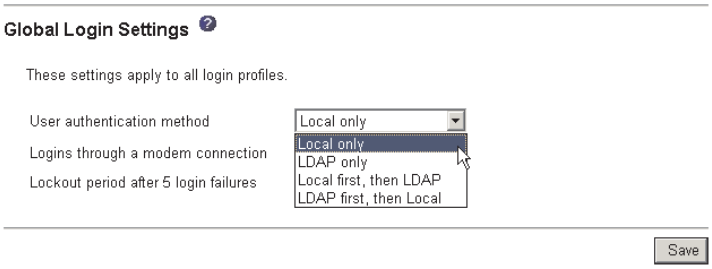
Some of the General Settings are used during SNMP and SMTP configuration. See “Configuring SNMP” on page 35 and “Configuring SMTP” on page 37 for additional information.

Login Profiles



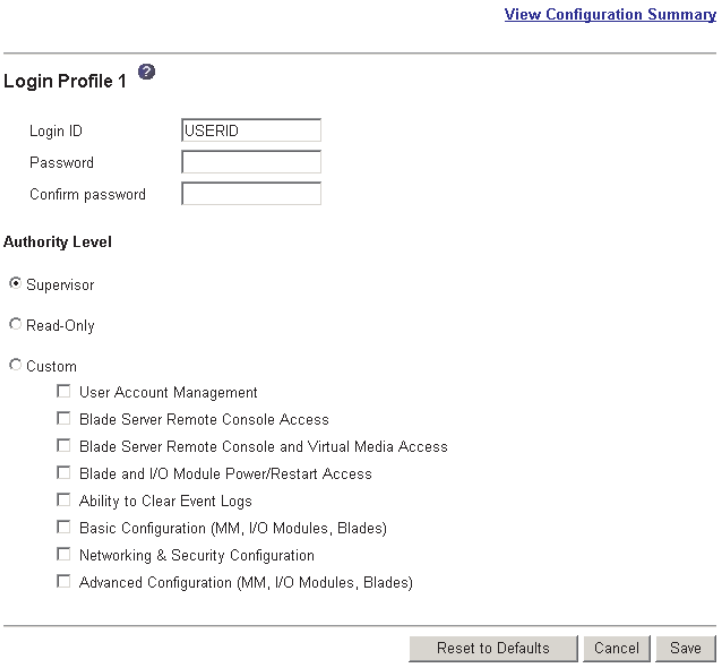
Select the Login Profiles choice to configure up to 12 login profiles for logging in to the management module; and to specify the following global login settings:

- User authentication method (local, LDAP, or both)
- How to process users that login using a modem
- Lockout period after five unsuccessful login attempts



For each user profile, specify the following values:

- Login ID
- Authority level (default is Read Only)
- Password (requires confirmation)

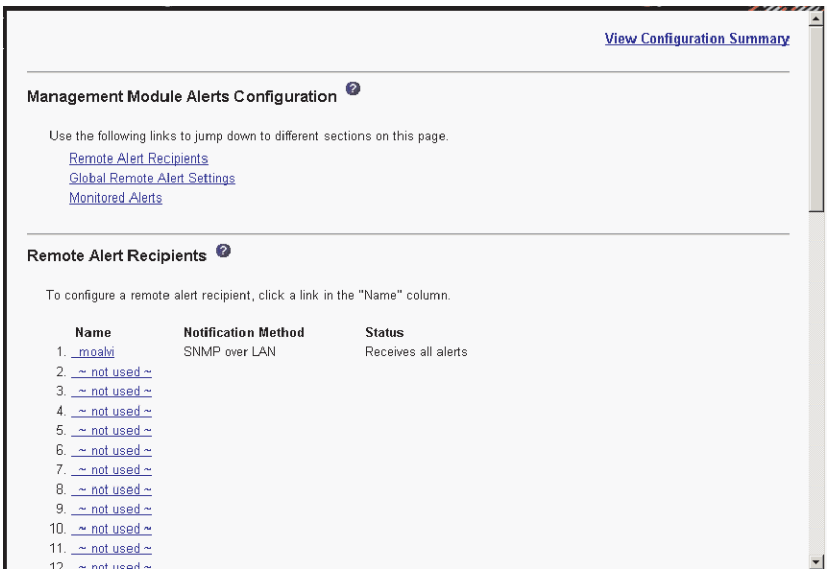


Several authority levels are available, each giving a user write and execute access to different areas of management-module function. Multiple authority levels can be assigned to each user. Users with Supervisor authority have write and execute access to all management-module functions. Users with Read-Only authority can access all management module functions for viewing only.

Attention: If you change the default login profile on your management module, be sure to keep a record of your login ID and password in a safe place. If you forget the management-module login ID and password, you must replace the management module.

Click on **View Configuration Summary** to display the configuration settings for all BladeCenter users and components.

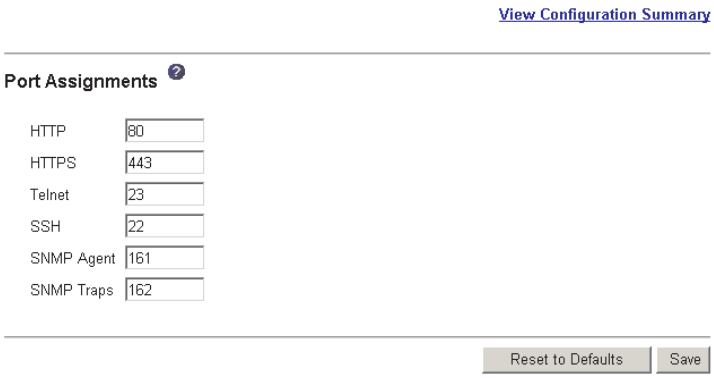
Alerts



Select the Alerts choice to specify which alerts (from lists of Critical, Warning, and System alerts) are monitored, which alert notifications are sent to whom, how alert notifications are sent (SNMP, e-mail, IBM Director), whether to include the event log with the notification, and other alert parameters.

Note: The IBM Director program is a system-management product that comes with the BladeCenter unit. To configure the remote alert recipients for IBM Director over LAN, the remote alert recipient must be an IBM Director-enabled server.

Port Assignments



Select the Port Assignments choice to configure some of the ports used by the management module. Management-module ports that can be configured on the Port Assignments screen are listed in Table 2.

Table 2. User configurable management-module ports

Port name	Default port number	Description
HTTP	80	Port used for Web server HTTP connection using UDP
HTTPS	443	Port used for SSL connection using TCP
Telnet	23	Port used for the Telnet command-line interface connection

Table 2. User configurable management-module ports (continued)

Port name	Default port number	Description
SSH	22	Port used for the Secure Shell (SSH) command-line interface connection
SNMP Agent	161	Port used for SNMP get/set commands using UDP
SNMP Traps	162	Port used for SNMP traps using UDP

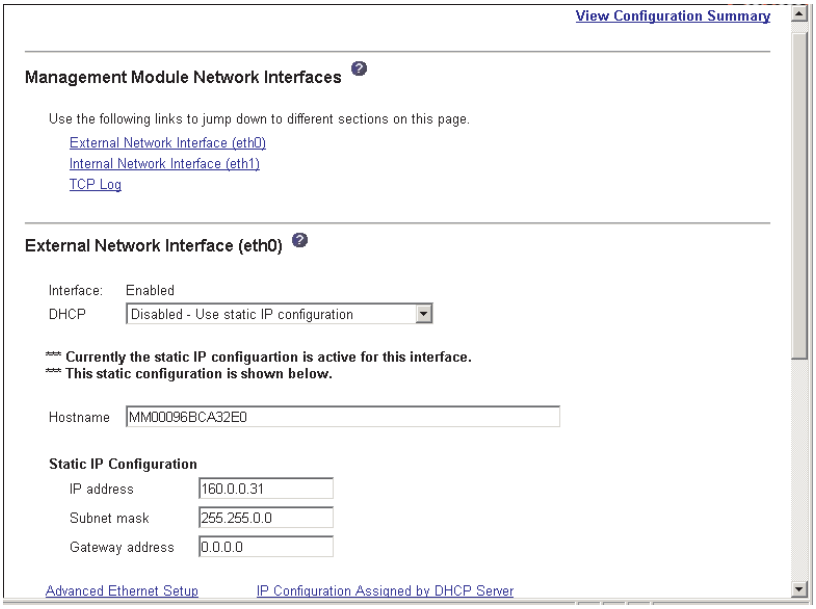
Other ports used by the management module are listed in Table 3. These ports are fixed and can not be modified by the user.

Table 3. Fixed management-module ports

Port number (fixed)	Description
25	Port used for TCP e-mail alerts
53	Port used for the UDP Domain Name Server (DNS) resolver
68	Port used for DHCP client connection using UDP
427	Port used for the UDP Service Location Protocol (SLP) connection
1044	Port used for remote disk function
1045	Port used for persistent remote disk (disk on card).
5900	Port used for the TCP VNC server applet
6090	Port used for IBM Director commands using TCP/IP
13991	Port used for IBM Director alerts using UDP

Click on **View Configuration Summary** to display the configuration settings for all BladeCenter users and components.

Network Interfaces



Select the Network Interfaces choice to configure the two management-module Ethernet interfaces: external (remote management and console), and internal (communication with the I/O modules). You can also select this choice to view the TCP log.

Notes:

1. When you use the management module Web interface to update an I/O module configuration, the management module firmware writes its settings for the I/O module only to the management module NVRAM; it does not write its settings for the I/O module to the I/O module NVRAM.

   If the I/O module restarts when the management module is not able to apply the IP address it has in NVRAM for the I/O module, the I/O module will use whatever IP address it has in its own NVRAM. If the two IP addresses are not the same, you might not be able to manage the I/O module any more. The management module cannot apply the I/O module IP address from its NVRAM if:

   - The management module is restarting
   - The management module has failed
   - The management module has been removed from the chassis

   You must use the Telnet interface to log into the I/O module, change the IP address to match the one you assigned through the management module, and then save the I/O module settings in the Telnet session (**Basic Setup → Save Changes**).
2. For I/O module communication with a remote management station, such as the IBM Director server, through the management module external Ethernet port, the I/O module internal network interface and the management module internal and external interfaces must be on the same subnet.

- **External Network Interface (eth0)** - This is the interface for the remote management and console port.

  Note: If you plan to use redundant management modules and want both to use the same external IP address, disable DHCP and configure and use the static IP address. (The IP configuration information will be transferred to the redundant management module automatically when needed.)

  – **Interface** - The status (Enabled or Disabled) of the Ethernet connection. The default is Enabled.

  – **DHCP** - Select one of the following choices:

    - **Try DHCP server. If it fails, use static IP config.** (this is the default).
    - **Enabled - Obtain IP config. from DHCP server**
    - **Disabled - Use static IP configuration**

  – **Hostname** - (Optional) This is the IP host name you want to use for the management module (maximum of 63 characters).

  – **Static IP configuration** - You need to configure this information only if DHCP is disabled.

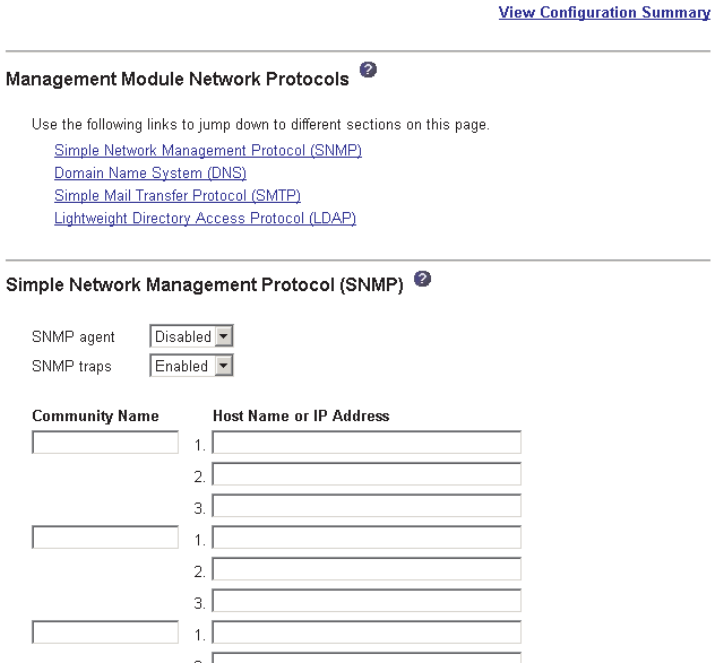
    - **IP address** - The IP address for the management module. The IP address must contain four integers from 0 to 255, separated by periods, with no spaces or consecutive periods. The default setting is 192.168.70.125.
    - **Subnet mask** - The subnet mask must contain four integers from 0 to 255, separated by periods, with no spaces. The default setting is 255.255.255.0
    - **Gateway address** - The IP address for your network gateway router. The gateway address must contain four integers from 0 to 255, separated by periods, with no spaces.

- **Internal Network Interface (eth1)** - This interface communicates with the network-interface I/O modules, such as an Ethernet I/O module or the Fibre Channel I/O module.
  - Specify the IP address to use for this interface. The subnet mask must be the same as the subnet mask in the external network interface (eth0).
  - View the data rate, duplex mode, maximum transmission unit (MTU), locally-administered MAC address, and burned-in MAC address for this interface. You can configure the locally-administered MAC address; the other fields are read-only.
- **TCP log** - Select this choice to view entries that are currently stored in the management module TCP log. This log contains error and warning messages generated by the TCP/IP code running on the management module, and might be used by your service representative for advanced troubleshooting. The log displays the most recent entries first.

  You can sort and filter entries in the event log.

Click on **View Configuration Summary** to display the configuration settings for all BladeCenter users and components.

Network Protocols

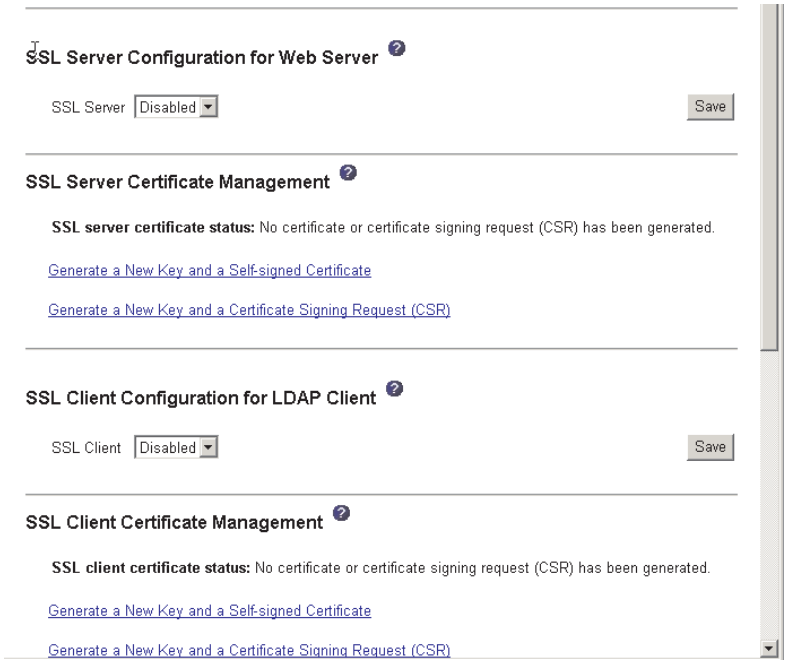


Select the Network Protocols choice to view or change the settings for the SNMP, DNS, SMTP, and LDAP protocols.

Click on **View Configuration Summary** to display the configuration settings for all BladeCenter users and components.

Some of the Network Protocol settings are used during SNMP, SMTP, and LDAP configuration. See “Configuring SNMP” on page 35, “Configuring SMTP” on page 37, and “Configuring LDAP” on page 38 for additional information.

Security



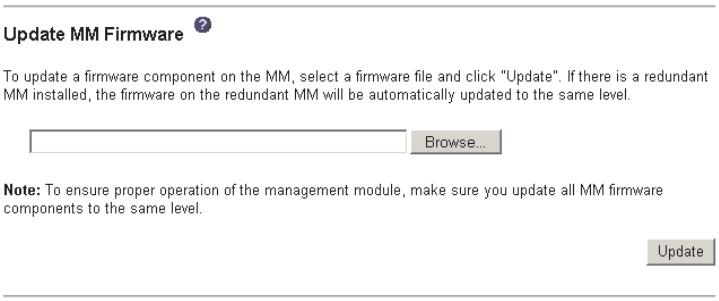
Select the Security choice to view or change the secure socket layer (SSL) settings for the Web server and LDAP client, and view or change the Web server secure shell (SSH) settings. You can enable or disable (the default) SSL, and choose between self-signed certificates and certificates provided by a certificate authority (CA). You can also enable or disable (the default) SSH, and generate and manage the SSH server key.

Some of the Security settings are used during SSL, LDAP, and SSH configuration. See “Secure Web server and secure LDAP” on page 42 and “Configuring the secure shell server” on page 52 for additional information.

Configuration File

Select the Configuration File choice to back up or restore the management-module configuration file. See “Using the configuration file” on page 54 for instructions.

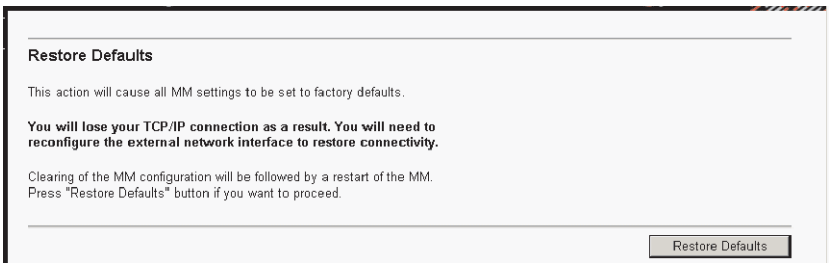
Firmware Update



Select the Firmware Update choice to update the management-module firmware; if a second management module is installed, the firmware update will automatically be applied to both management modules. Click **Browse** to locate the firmware file you want; then, click **Update**.

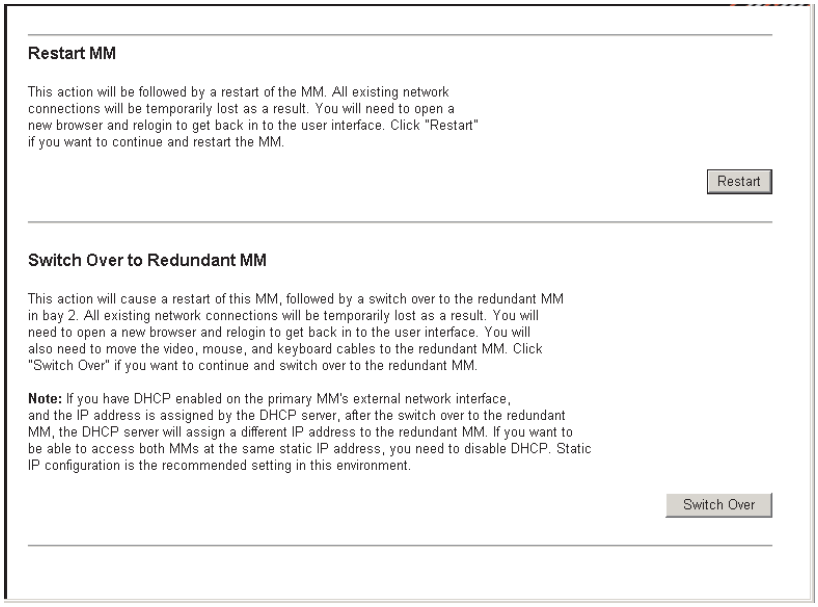
Management-module firmware is in several separate files that are installed independently; you must install all of the firmware update files. You can obtain the firmware files from the IBM Support Web site at http://www.ibm.com/pc/support/.

Restore Defaults



Select the Restore Defaults choice to restore the factory default configuration of the management module.

Restart MM



Select the Restart MM choice to restart (reset) the management module. If a second management module is present, select this choice to change to the redundant management module.

Network and security configuration

The following sections describe how to configure management module networking and security parameters for:

- SNMP and DNS (see “Configuring SNMP”)
- SMTP (see “Configuring SMTP” on page 37)
- SSL and LDAP (see “Configuring LDAP” on page 38)
- SSH (see “Configuring the secure shell server” on page 52)

Configuring SNMP

You can query the SNMP agent to collect the sysgroup information and to send configured SNMP alerts to the configured host names or IP addresses.

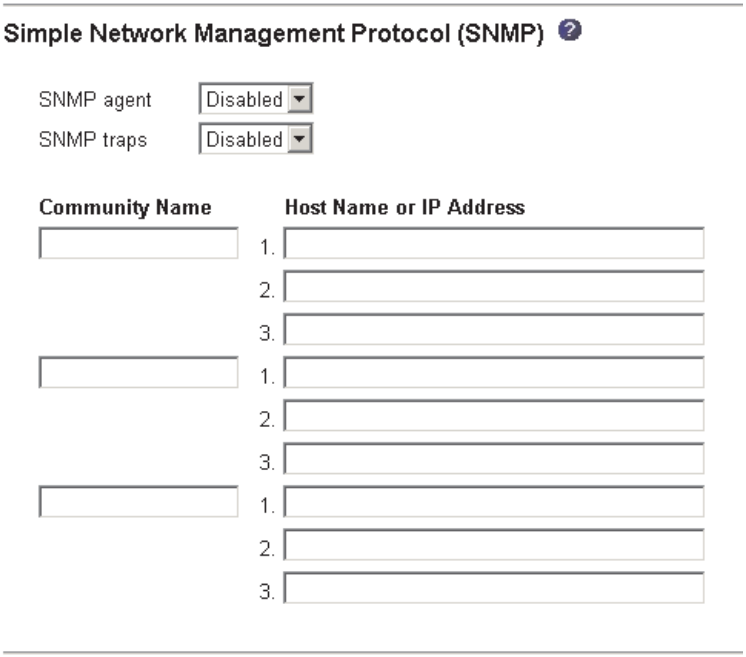
Note: If you plan to configure Simple Network Management Protocol (SNMP) traps on the management module, you must install and compile the management information base (MIB) on your SNMP manager. The MIB supports SNMP traps. The MIB is included in the management-module firmware update package that you downloaded from the IBM Support Web site.

Complete the following steps to configure your SNMP:

1. Log in to the management module where you want to configure SNMP. For more information, see “Starting the management-module Web interface” on page 12
2. In the navigation pane, click **MM Control → General Settings**. In the management-module information page that opens, specify the following information:

- **Management module name** - The name that you want to use to identify the management module. The name will be included with e-mail and SNMP alert notifications to identify the source of the alert.
- **System contact** - The name and phone number of the person to contact if there is a problem with the BladeCenter unit.
- **System location** - Sufficient detail to quickly locate the BladeCenter unit for maintenance or other purposes.

3. Scroll to the bottom of the page and click **Save**.
4. In the navigation pane, click **MM Control → Network Protocols**; then, click the **Simple Network Management Protocol (SNMP)** link. A page similar to the one in the following illustration is displayed.



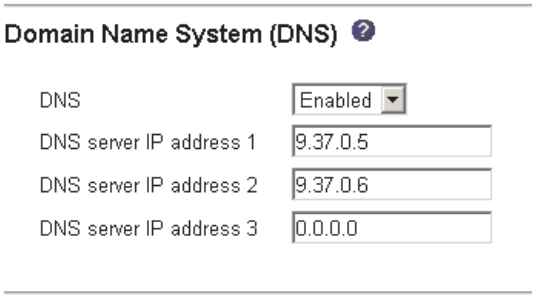
5. Select **Enabled** in the **SNMP agent** and **SNMP traps** fields to forward alerts to SNMP communities on your network. To enable the SNMP agent, the following criteria must be met:
   - System contacts must be specified on the General Settings page.
   - The system location must be specified on the General Settings page.
   - At least one community name must be specified.
   - At least one valid IP address or host name (if DNS is enabled) must be specified for that community.

   Note: Alert recipients whose notification method is SNMP will not receive alerts unless both the SNMP agent and the SNMP traps are enabled.
6. Set up a community to define the administrative relationship between SNMP agents and SNMP managers. You must define at least one community. Each community definition consists of the following parameters:
   - Name
   - IP address

   If either of these parameters is not correct, SNMP management access is not granted.

Note: If an error message window opens, make the necessary adjustments to the fields listed in the error window. Then, scroll to the bottom of the page and click **Save** to save your corrected information. You must configure at least one community to enable this SNMP agent.

7. In the **Community Name** field, enter a name or authentication string to specify the community.
8. In the corresponding **Host Name** or **IP Address** field, enter the host name or IP addresses of each community manager.
9. If a DNS server is not available on your network, scroll to the bottom of the page and click **Save**.
10. If a DNS server is available on your network, scroll to the **Domain Name System (DNS)** section. A page similar to the one in the following illustration is displayed.



11. If a DNS server (or servers) is available on your network, select **Enabled** in the **DNS** field. The **DNS** field specifies whether you use a DNS server on your network to translate host names into IP addresses.
12. If you enabled DNS, in the **DNS server IP address** fields, you can specify the IP addresses of up to three DNS servers on your network. Each IP address should contain integers from 0 through 255, separated by periods.
13. Scroll to the bottom of the page and click **Save**.
14. In the navigation pane, click **MM Control → Restart MM** to activate the changes.

Configuring SMTP

Complete the following steps to specify the IP address or host name of the Simple Mail Transfer Protocol (SMTP) server.

Note: If you plan to set up an SMTP server for e-mail alert notifications, be sure that the name in the **Name** field in the **MM Information** section of the MM Control → General Settings window is valid as part of an e-mail address (for example, there are no spaces).

1. Log in to the management module where you want to configure SMTP. For more information, see “Starting the management-module Web interface” on page 12.
2. In the navigation pane, click **MM Control → Network Protocols** and scroll down to the **Simple Mail Transfer Protocol (SMTP)** section.

3. In the **SMTP Server Host Name or IP Address** field, type the host name of the SMTP server. Use this field to specify the IP address or, if DNS is enabled and configured, the host name of the SMTP server.
4. Scroll to the bottom of the page and click **Save**.

Configuring LDAP

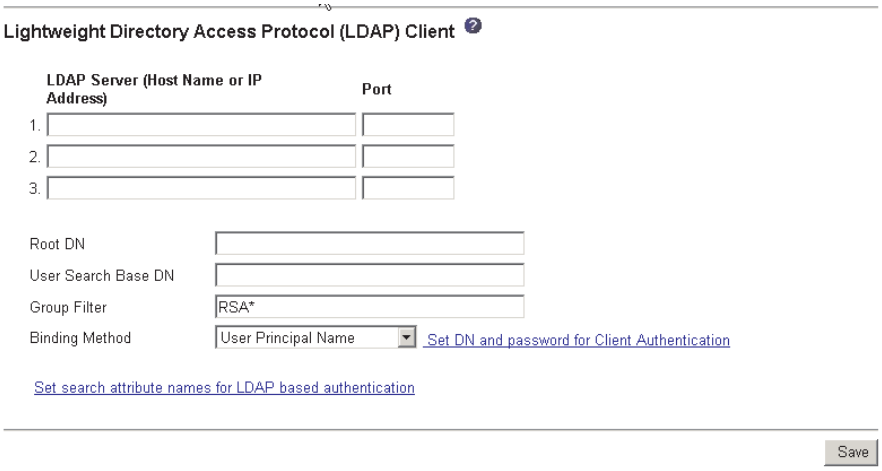
Using a Lightweight Directory Access Protocol (LDAP) server, a management module can authenticate a user by querying or searching an LDAP directory on an LDAP server, instead of going through its local user database. Then, all LDAP clients (BladeCenter management modules or server remote supervisor adapters) can remotely authenticate any user access through a central LDAP server. This requires LDAP client support on the management module. You can also assign authority levels based on information found on the LDAP server.

You can also use LDAP to assign users and management modules to groups, and perform group authentication, in addition to the normal user (password check) authentication. For example, a management module can be associated with one or more groups, and a user would only pass group authentication if he belongs to at least one group associated with the management module.

Setting up a client to use the LDAP server

Complete the following steps to set up a client to use the LDAP server:

1. Log in to the management module where you want to set up the client. For more information, see “Starting the management-module Web interface” on page 12.
2. In the navigation pane, click **MM Control → Network Protocols**. Scroll down to the **Lightweight Directory Access Protocol (LDAP) Client** section. A page similar to the one in the following illustration is displayed.



3. Configure the LDAP client using the following information:

   LDAP Server

   The management module contains a Version 2.0 LDAP client that you can configure to provide authentication through a centrally located LDAP server. You can configure up to three LDAP servers. The port number for each server is optional. If left blank, the default value of 389 is used for non-secured LDAP connections. For secured connections, the default is 636. You must configure at least one LDAP server.

Root DN

The distinguished name for the root entry of the directory tree on the LDAP server. An example might look like dn=companyABC,dn=com.

User Search Base DN

As part of the user authentication process, it is necessary to search the LDAP server for one or more attributes associated with a particular user. Any search request must specify the base distinguished name for the actual search. The **User Search Base DN** field specifies the base distinguished name that is used to search the user directory. An example might look like cn=Users,dn=companyABC,dn=com. If this field is left blank, the root distinguished name is used as the search base.

User searches are part of the authentication process. They are carried out to retrieve information about the user such as login permissions, callback number, and group memberships. For Version 2.0 LDAP clients, be sure to configure this parameter; otherwise, a search using the root distinguished name might not succeed (as seen on Microsoft Windows® Server 2003 Active Directory servers).

ASM Group Filter

This parameter is used for group authentication. It specifies the set of groups to which this particular management module belongs. If left blank, group authentication is disabled. Otherwise, group authentication is performed against this filter. The filter specified can be a specific group name (for example, RSAWest), a wildcard with a prefix (for example, RSA*), or a wildcard (specified as *). If a specific name is used, this management module belongs only to this group. If a prefix filter is used (for example, RSA*), this management module belongs to any group whose first three letters are RSA. If a wildcard filter (*) is used, then this management module belongs to all groups. The default filter is RSA*.

Group authentication is performed after user authentication (where a user ID and password are verified). Group authentication refers to the process of verifying that a user is a member of at least one group associated with this management module. For example, assume the group filter is set to RSA*. If the user belongs to two groups, for example, Engineering and RSAWest, group authentication passes because the user belongs to a group (RSAWest) that matches the filter RSA*. If the groups to which the user belong do not match the filter, group authentication fails and the user is not allowed to access the management module. Note that if the group filter is *, then group authentication will automatically succeed because any group to which the user belongs will match this wildcard.

Binding Method

For initial binds to the LDAP server during user authentication, choose from the following options:

Anonymous authentication. A bind attempt is made without a client distinguished name or password. If the bind is successful, a search will be requested to find an entry on the LDAP server for the user attempting to log in. If an entry is found, a second attempt to bind will be attempted, this time with the distinguished name and password of the user. If this succeeds, the user has passed the user authentication phase. Group authentication is then attempted if it is enabled.

Client authentication. A bind attempt is made with the client distinguished name and password specified by this configuration parameter. If the bind is successful, the user authentication phase proceeds as in Anonymous authentication.

User Principal Name. A bind attempt is made directly with the credentials used during the login process. If this succeeds, the user has passed the user authentication phase. The user principal name usually refers to a fully qualified name, such as johndoe@abc.com. However, johndoe would also be acceptable.

Strict User Principal Name. This is similar to the user principal name, except that a fully qualified name must be entered by the user. That is, johndoe@abc.com would be acceptable, but not johndoe. The name entered by the user will be parsed for the @ symbol.

Configuring the LDAP client authentication

Complete the following steps to configure the LDAP client authentication:

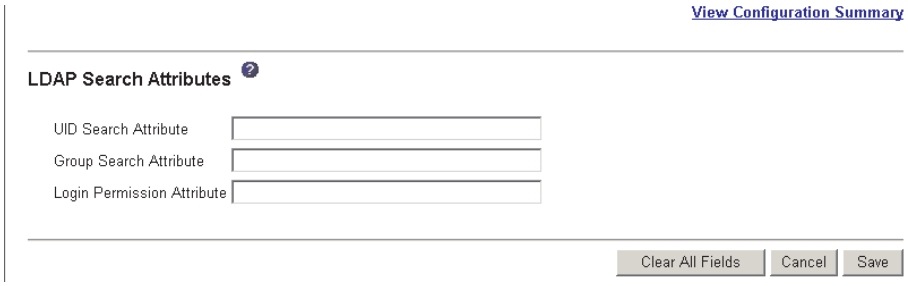
1. In the navigation pane, click **MM Control → Network Protocols**.
2. Scroll down to the **Lightweight Directory Access Protocol (LDAP) Client** section and click **Set DN and password for Client Authentication**. A page similar to the one in the following illustration is displayed.

3. The initial bind to the LDAP server during user authentication can be performed with anonymous authentication, client-based authentication, or user principle name. To use client-based authentication, in the **Client DN** field, type a client distinguished name. Type a password in the **Password** field or leave it blank.

Configuring the LDAP search attributes

Complete the following steps to configure the LDAP search attributes:

1. In the navigation pane, click **MM Control → Network Protocols**.
2. Scroll down to the Lightweight Directory Access Protocol (LDAP) Client section and click **Set search attribute names for LDAP based authentication**. A page similar to the one in the following illustration is displayed.



3. To configure the search attributes, use the following information.

UID Search Attribute

When the binding method selected is Anonymous authentication or Client authentication, the initial bind to the LDAP server is followed by a search request directed at retrieving specific information about the user, including the distinguished name, login permissions, and group ownerships of the user. To retrieve this information, the search request must specify the attribute name used to represent user IDs on that server. Specifically, this name is used as a search filter against the login ID entered by the user. This attribute name is configured here. If this field is left blank, a default of UID is used during user authentication. For example, on Active Directory servers, the attribute name used for user IDs is often sAMAccoutName.

When the binding method selected is User principal name or Strict user principal name, the **UID Search Attribute** field defaults automatically to userPrincipalName during user authentication if the user ID entered has the form userid@somedomain.

Group Search Attribute

When the Group Filter name is configured, it is necessary to retrieve from the LDAP server the list of groups to which a particular user belongs. This is required to perform group authentication. To retrieve this list, the search filter sent to the server must specify the attribute name associated with groups. This field specifies this attribute name.

If this field is left blank, the attribute name in the filter will default to memberOf.

Login Permission Attribute

When a user is successfully authenticated using an LDAP server, the login permissions for this user must be retrieved. To retrieve these permissions, the search filter sent to the server must specify the attribute name associated with login permissions. This field specifies this attribute name.

If this field is left blank, the user is assigned a default of read-only permissions, assuming user and group authentication passes. When successfully retrieved, the attribute value returned by the LDAP server is interpreted according to the following information:

- It must be a bit string entered as 12 consecutive zeros or ones, with each bit representing a particular set of functions. For example: 010000000000 or 000011001000. The bits are numbered according to their position. The leftmost bit is bit position 0, and the rightmost bit is bit position 11. A value of 1 at a particular position enables that particular function. A value of 0 disables that function. There are 12 available bits, which are described in the following list:
  - Deny Always (bit position 0): If set, a user will always fail authentication. This function can be used to block a particular user or users associated with a particular group.
  - Supervisor Access (bit position 1): If set, a user is given administrator privileges. The user has read and write access to every function. When this bit is set, the other bits below do not have to be set individually.
  - Read Only Access (bit position 2): If set, a user has read-only access and cannot perform any maintenance procedures (for example, restart, remote actions, and firmware updates), and nothing can be modified (using the save, clear, or restore functions). Note that

read-only and all other bits are mutually exclusive, with read-only having the lowest precedence. That is, if any other bit is set, this bit will be ignored.

  - Networking and Security (bit position 3): If set, a user can modify the settings in the Security, Network Protocols, and Network Interface pages for MM Control. If set, a user can also modify the settings in the Management page for I/O Module Tasks.
  - User Account Management (bit position 4): If set, a user can add, modify, and delete users and change the Global Login Settings in the Login Profiles page.
  - Blade server Remote Console Access (bit position 5): If set, a user can access the remote server console.
  - Blade server Remote Console and Virtual Media Access (bit position 6): If set, a user can access the remote server console and the virtual media functions for the remote server.
  - Blade and I/O Module Power/Restart Access (bit position 7): If set, a user can access the power on and restart functions for the remote blades servers and I/O Modules. These functions are available in the Power/Restart pages.
  - Basic Configuration (MM, I/O Modules, Blades) (bit position 8): If set, a user can modify the General Settings and Alerts pages for MM Control, and the Configuration page for Blade Tasks.
  - Ability to Clear Event Logs (bit position 9): If set, a user can clear the event logs. Everyone can look at the event logs, but this particular permission is required to clear the logs.
  - Advanced Configuration (MM, I/O Modules, Blades (bit position 10): If set, a user has no restrictions when configuring the management module, blade servers, I/O Modules, and VPD. This user can also perform firmware upgrades on the management module or blade servers, restore the management module to its factory default settings, modify and restore the management-module configuration from a configuration file, and restart or reset the management module.
  - Reserved (bit position 11): Reserved for future use.

- If none of the bits are set, the default will be set to read-only for the user.
- Priority is given to login permissions retrieved directly from the user record. If the user does not have the login permission attribute in its record, an attempt will be made to retrieve the permissions from the groups to which the user belongs. This is done as part of the group authentication phase. The user will be assigned the inclusive OR of all the bits for all of the groups. The Browser Only bit will be set only if all the other bits are zero. If the Deny Always bit is set for any of the groups, the user will be refused access. The Deny Always bit always has precedence over every other bit.

Secure Web server and secure LDAP

Secure Sockets Layer (SSL) is a security protocol that provides communication privacy. SSL enables applications to communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

You can configure the management module to use SSL support for two types of connections: secure Web server (HTTPS) and secure LDAP connection (LDAPS). The management module takes on the role of SSL client or SSL server depending on the type of connection. The following table shows that the management module

acts as an SSL server for secure Web server connections. The management module acts as an SSL client for secure LDAP connections.

Table 4. Management module SSL connection support

Connection type	SSL client	SSL server
Secure Web server (HTTPS)	Web browser of the user (For example: Microsoft Internet Explorer)	Management-module Web server
Secure LDAP connection (LDAPS)	Management-module LDAP client	An LDAP server

You can view or change the Secure Sockets Layer (SSL) settings from the MM Control → Security page. You can enable or disable SSL and manage the certificates required for SSL.

Configuring security

Use the general procedure in this section to configure security for the management module Web server and to configure security for the connection between the management module and an LDAP server. If you are not familiar with the use of SSL certificates, read the information in "SSL certificate overview" on page 44.

The content of the Security Web page is context-sensitive. The selections available on the page change when certificates or certificate signing requests are generated, when certificates are imported or removed, and when SSL is enabled or disabled for the client or the server.

Use the following general tasks list to configure the security for the management module:

1. Configure the Secure Web server:
   a. Disable the SSL server. Use the **SSL Server Configuration for Web Server** section on the MM Control → Security page.
   b. Generate or import a certificate. Use the **SSL Server Certificate Management** section on the MM Control → Security page. (See "SSL server certificate management" on page 44.)
   c. Enable the SSL server. Use the **SSL Server Configuration for Web Server** section on the MM Control → Security page. (See "Enabling SSL for the secure Web server" on page 50.)
2. Configure SSL security for LDAP connections:
   a. Disable the SSL client. Use the **SSL Client Configuration for LDAP Client** section on the MM Control → Security page.
   b. Generate or import a certificate. Use the **SSL Client Certificate Management** section on the MM Control → Security page. (See "SSL client certificate management" on page 50.)
   c. Import one or more trusted certificates. Use the **SSL Client Trusted Certificate Management** section on the MM Control → Security page. (See "SSL client trusted certificate management" on page 50.)
   d. Enable the SSL client. Use the **SSL Client Configuration for LDAP Client** section on the MM Control → Security page. (See "Enabling SSL for the LDAP client" on page 52.)
3. Restart the management module for SSL server configuration changes to take effect. For more information, see "Restart MM" on page 35.

Note: Changes to the SSL client configuration take effect immediately and do not require a restart of the management module.

SSL certificate overview

You can use SSL with either a self-signed certificate or with a certificate signed by a third-party certificate authority. Using a self-signed certificate is the simplest method for using SSL, but it does create a small security risk. The risk arises because the SSL client has no way of validating the identity of the SSL server for the first connection attempted between the client and server. It is possible that a third party could impersonate the server and intercept data flowing between the management module and the Web browser. If at the time of the initial connection between the browser and the management module, the self-signed certificate is imported into the certificate store of the browser, all future communications will be secure for that browser (assuming the initial connection was not compromised by an attack).

For more complete security, you can use a certificate signed by a certificate authority. To obtain a signed certificate, use the SSL Certificate Management page to generate a certificate signing request. You must then send the certificate signing request to a certificate authority and make arrangements to procure a certificate. When the certificate is received, it is then imported into the management module using the **Import a Signed Certificate** link, and you can enable SSL.

The function of the certificate authority is to verify the identity of the management module. A certificate contains digital signatures for the certificate authority and the management module. If a well-known certificate authority issues the certificate or if the certificate of the certificate authority has already been imported into the Web browser, the browser will be able to validate the certificate and positively identify the management-module Web server.

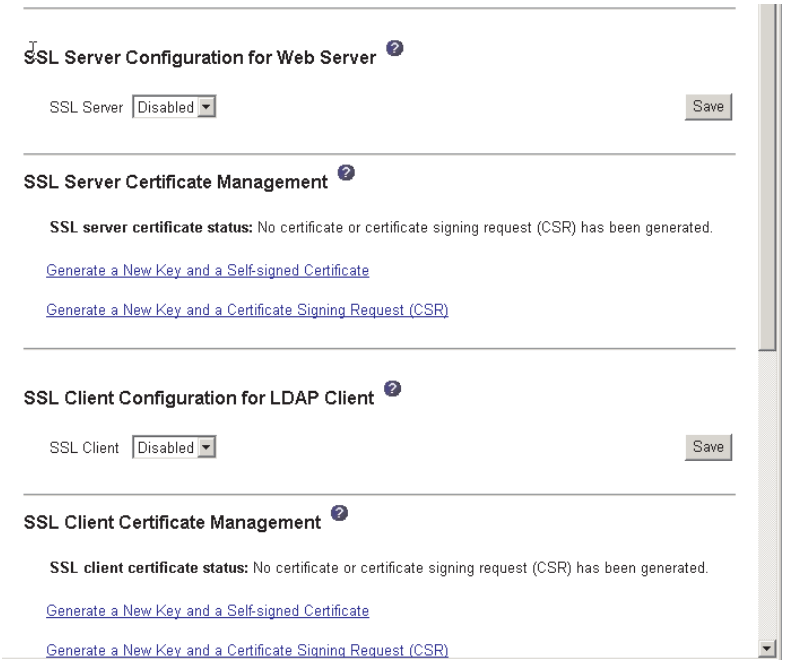
The management module requires a certificate for the secure Web server and one for the secure LDAP client. Also, the secure LDAP client requires one or more trusted certificates. The trusted certificate is used by the secure LDAP client to positively identify the LDAP server. The trusted certificate is the certificate of the certificate authority that signed the certificate of the LDAP server. If the LDAP server uses self-signed certificates, the trusted certificate can be the certificate of the LDAP server itself. Additional trusted certificates can be imported if more than one LDAP server is used in your configuration.

SSL server certificate management

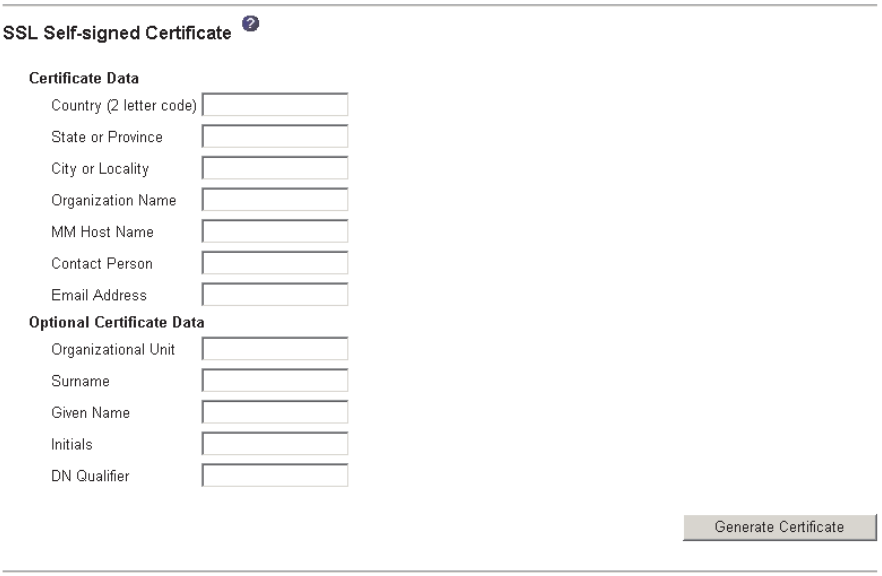
The SSL server requires that a valid certificate and corresponding private encryption key is installed before SSL is enabled. There are two methods available for generating the private key and required certificate: using a self-signed certificate and using a certificate signed by a certificate authority. If you want to use a self-signed certificate for the SSL server, see “Generating a self-signed certificate” on page 45. If you want to use a certificate authority signed certificate for the SSL server, see “Generating a certificate signing request” on page 46.

Generating a self-signed certificate: Complete the following steps to generate a new private encryption key and self-signed certificate:

1. In the navigation plane, click **MM Control → Security**. A page similar to the one in the following illustration is displayed.



2. In the SSL Server Configuration for Web Server section, make sure that the SSL server is disabled. If it is not disabled, select **Disabled** in the **SSL Server** field and then click **Save**.
3. In the SSL Server Certificate Management section, select **Generate a New Key and a Self-signed Certificate**. A page similar to the one in the following illustration is displayed.



4. Type the information in the required fields and any optional fields that apply to your configuration. For a description of the fields, see “Required certificate data”

on page 46. After you finish typing the information, click **Generate Certificate**. Your new encryption keys and certificate are generated. This process might take several minutes.

A page similar to the one in the following illustration is displayed and you can see that a self-signed certificate is installed.

Generating a certificate signing request: Complete the following steps to generate a new private encryption key and certificate signing request:

1. In the navigation pane, click **MM Control → Security**.
2. In the SSL Server Configuration for Web Server section, make sure that the SSL server is disabled. If it is not disabled, select **Disabled** in the **SSL Server** field and then click **Save**.
3. In the SSL Server Certificate Management section, select **Generate a New Key and a Certificate Signing Request**. A page similar to the one in the following illustration is displayed.

4. Type the information in the required fields and any optional fields that apply to your configuration. The fields are the same as the self-signed certificate with some additions.

   Read the information in the following sections for a description of each of the common fields.

   Required certificate data

   The following user-input fields are required for generating a self-signed certificate or a certificate signing request.

Country

Use this field to indicate the country where the management module physically resides. This field must contain the 2-character country code.

State or Province

Use this field to indicate the state or province where the management module physically resides. This field can contain a maximum of 30 characters.

City or Locality

Use this field to indicate the city or locality where the management module physically resides. This field can contain a maximum of 50 characters.

Organization Name

Use this field to indicate the company or organization that owns the management module. When this is used to generate a certificate signing request, the issuing certificate authority can verify that the organization requesting the certificate is legally entitled to claim ownership of the given company or organization name. This field can contain a maximum of 60 characters.

MM Host Name

Use this field to indicate the management module host name that currently appears in the browser Web address bar.

Make sure that the value you typed in the **MM host name** field exactly matches the host name as it is known by the Web browser. The browser compares the host name in the resolved Web address to the name that appears in the certificate. To prevent certificate warnings from the browser, the value used in this field must match the host name used by the browser to connect to the management module. For example, if the Web address bar in the browser currently is http://mm11.xyz.com/private/main.ssi, the value used for the **MM Host Name** field must be mm11.xyz.com. If the Web address is http://mm11/private/main.ssi, the value used must be mm11. If the Web address is http://192.168.70.2/private/main.ssi, the value used will be 192.168.70.2.

This certificate attribute is generally referred to as the common name.

This field can contain a maximum of 60 characters.

Contact Person

Use this field to indicate the name of a contact person responsible for the management module. This field can contain a maximum of 60 characters.

Email Address

Use this field to indicate the e-mail address of a contact person responsible for the management module. This field can contain a maximum of 60 characters.

Optional certificate data

The following user-input fields are optional for generating a self-signed certificate or a certificate signing request.

Organizational Unit

Use this field to indicate the unit within the company or organization that owns the management module. This field can contain a maximum of 60 characters.

Surname

Use this field for additional information, such as the surname of a person responsible for the management module. This field can contain a maximum of 60 characters

Given Name

Use this field for additional information, such as the given name of a person responsible for the management module. This field can contain a maximum of 60 characters.

Initials

Use this field for additional information, such as the initials of a person responsible for the management module. This field can contain a maximum of 20 characters.

DN Qualifier

Use this field for additional information, such as a distinguished name qualifier for the management module. This field can contain a maximum of 60 characters.

Certificate signing request attributes

The following fields are optional unless they are required by your selected certificate authority.

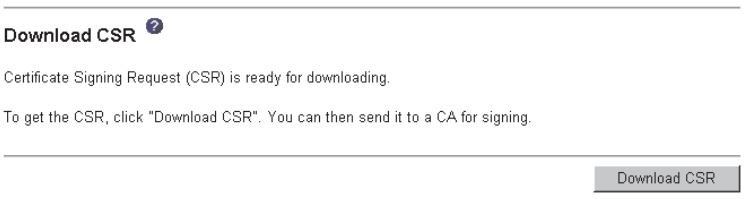
Challenge Password

Use this field to assign a password to the certificate signing request. This field can contain a maximum of 30 characters.

Unstructured Name

Use this field for additional information, such as an unstructured name assigned to the management module. This field can contain a maximum of 60 characters.

5. After completing the information, click **Generate CSR**. The new encryption keys and certificate are generated. This process might take several minutes. A page similar to the one in the following illustration is displayed when the process is completed.



6. Click **Download CSR** and then click **Save** to save the file to your workstation. The file produced when you create a certificate signing request is in DER format. If your certificate authority expects the data in some other format, such as PEM, the file can be converted using a third-party tool such as OpenSSL (http://www.openssl.org). If the certificate authority asks you to copy the contents of the certificate signing request file into a Web browser window, PEM format is usually expected.

   The command for converting a certificate signing request from DER to PEM format using OpenSSL is similar to the following:

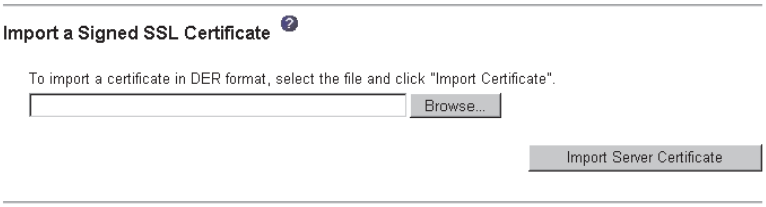
```
openssl req -in csr.der -inform DER -out csr.pem -outform PEM
```

7. Send the certificate signing request to your certificate authority. When the certificate authority returns your signed certificate it might be necessary to convert the certificate to DER format. (If you received the certificate as text in an e-mail or a Web page, it is probably in PEM format.) You can change the format using a tool provided by your certificate authority or using a third-party tool such as OpenSSL (http://www.openssl.org). The command for converting a certificate from PEM to DER format is similar to the following:

   ```
   openssl x509 -in cert.pem -inform PEM -out cert.der -outform DER
   ```

   Go to step 8 after the signed certificate is returned from the certificate authority.
8. In the navigation pane, click **MM Control → Security**. Scroll to the SSL Server Certificate Management section, which looks similar to the page in the following illustration.

9. Select **Import a Signed Certificate**. A page similar to the one in the following illustration is displayed.



10. Click **Browse**.
11. Click the certificate file that you want and then click **Open**. The file name (including the full path) is displayed in the field next to the **Browse** button.
12. Click **Import Server Certificate** to begin the process. A progress indicator is displayed as the file is transferred to storage on the management module. Remain on this page until the transfer is completed.

Enabling SSL for the secure Web server

Note: To enable SSL, you must have a valid SSL certificate installed.

Complete the following steps to enable the secure Web server:

1. In the navigation pane, click **MM Control → Security**. The page that is displayed looks similar to the one in the following illustration and shows that a valid SSL server certificate is installed. If the SSL server certificate status does not show that a valid SSL certificate is installed, go to “SSL server certificate management” on page 44.

2. Scroll to the SSL Server Configuration for Web Server section and select **Enabled** in the **SSL Client** field and then click **Save**. The value selected takes effect the next time the management module is restarted.

SSL client certificate management

The SSL client requires that a valid certificate and corresponding private encryption key is installed before SSL is enabled. There are two methods available for generating the private key and required certificate: using a self-signed certificate, or using a certificate signed by a certificate authority.

The procedure for generating the private encryption key and certificate for the SSL client is the same as the procedure for the SSL server, except that you use the SSL Client Certificate Management section of the Security Web page instead of the SSL Server Certificate Management section. If you want to use a self-signed certificate for the SSL client, see “Generating a self-signed certificate” on page 45. If you want to use a certificate authority signed certificate for the SSL client, see “Generating a certificate signing request” on page 46.

SSL client trusted certificate management

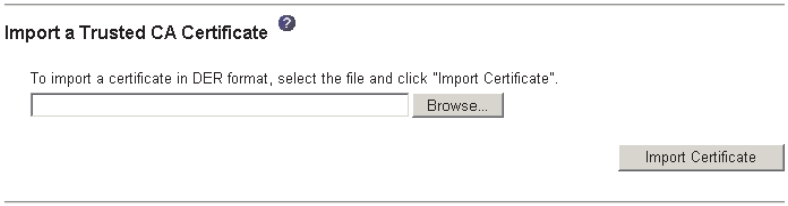
The secure SSL client (LDAP client) uses trusted certificates to positively identify the LDAP server. A trusted certificate can be the certificate of the certificate authority that signed the certificate of the LDAP server or it can be the actual certificate of the LDAP server. At least one certificate must be imported to the management module before the SSL client is enabled. You can import up to three trusted certificates.

Complete the following steps to import a trusted certificate:

1. In the navigation pane, select **MM Control → Security**.
2. In the SSL Client Configuration for LDAP Client section, make sure that the SSL client is disabled. If it is not disabled, select **Disabled** in the **SSL Client** field and then click **Save**.

3. Scroll to the SSL Client Trusted Certificate Management section. A page similar to the one in the following illustration is displayed.

4. Click **Import** next to one of the **Trusted CA Certificate 1** fields. A page similar to the one in the following illustration is displayed.



5. Click **Browse**.
6. Select the certificate file that you want and click **Open**. The file name (including the full path) is displayed in the box beside the **Browse** button.
7. To begin the import process, click **Import Certificate**. A progress indicator is displayed as the file is transferred to storage on the management module. Remain on this page until the transfer is completed.
8. The SSL Client Trusted Certificate Management section of the MM Control → Security page will now look similar to the one in the following illustration.

The **Remove** button is now available for the Trusted CA Certificate 1 option. If you want to remove a trusted certificate, click the corresponding **Remove** button.

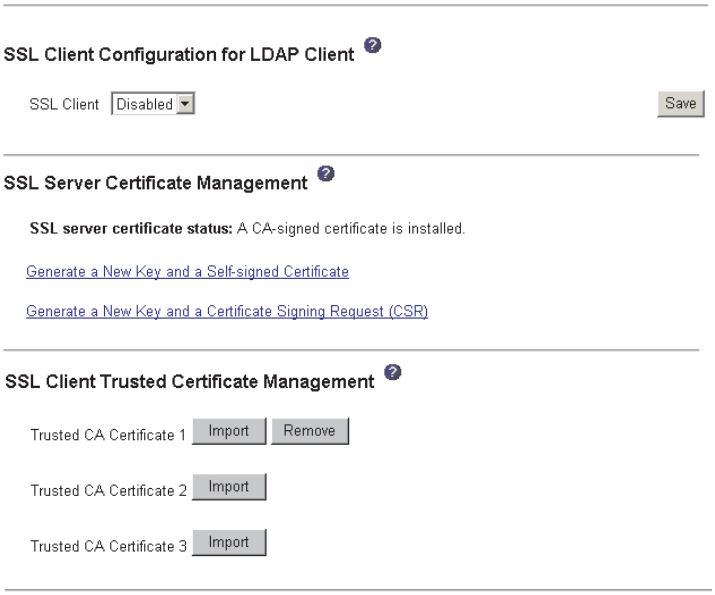
You can import other trusted certificates using the Trusted CA Certificate 2 and the Trusted CA Certificate 3 **Import** buttons.

Enabling SSL for the LDAP client

Use the SSL Client Configuration for LDAP Client section of the Security page to enable or disable SSL for the LDAP Client. To enable SSL, a valid SSL client certificate and at least one trusted certificate must first be installed.

Complete the following steps to enable SSL for the client:

1. In the navigation pane, click **MM Control → Security**. A page similar to the one in the following illustration is displayed.



   The MM Control → Security page shows an installed SSL client certificate and Trusted CA Certificate 1.
2. On the SSL Client Configuration for LDAP Client page, select **Enabled** in the **SSL Client** field.
3. Click **Save**. The value selected takes effect immediately.

Configuring the secure shell server

The Secure Shell (SSH) feature provides secure access to the command-line interface and the serial over LAN (text console) redirect features of the management module.

Secure shell users are authenticated by exchanging user ID and password. The password and user ID are sent after the encryption channel is established. The user ID and password pair can be one of the 12 locally stored user IDs and passwords or they can be stored on an LDAP server. Public key authentication is not supported.

Generating a secure shell server key

A secure shell server key is used to authenticate the identity of the secure shell server to the client. Secure shell must be disabled before you create a new secure shell server private key. You must create a server key before enabling the secure shell server.

When you request a new server key, both a Rivest, Shamir, and Adelman (RSA) key and a DSA key are created to allow access to the management module from

either a SSH version 1.5 or SSH version 2 client. For security, the secure shell server private key is not backed-up during a configuration save and restore operation.

The following third-party SSH clients are available. While some SSH clients have been tested, support or non-support of any particular SSH client is not implied.

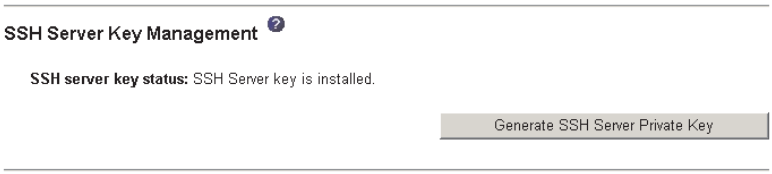
- The SSH clients distributed with operating systems such as Linux, AIX®, and UNIX® (see your operating-system documentation for information). The SSH client of Red Hat Linux 7.3 was used to test the command-line interface.
- The SSH client of cygwin (see http://www.cygwin.com for information)

The following table shows the types of encryption algorithms that are supported, based on the SSH version that is being used.

Algorithm	SSH version 1.5 clients	SSH version 2.0 clients
Public key exchange	SSH 1-key exchange algorithm	Diffie-Hellman-group 1-sha-1
Host key type	RSA (1024-bit)	DSA (1024-bit)
Bulk cipher algorithms	3-des	3-des-cbc or blowfish-cbc
MAC algorithms	32-bit crc	Hmac-sha1

Complete the following steps to create a new secure shell server key:

1. In the navigation pane, click **MM Control → Security**.
2. Scroll to the Secure Shell (SSH) Server section and make sure that the secure shell server is disabled. If it is not disabled, select **Disabled** in the **SSH Server** field and then click **Save**.
3. Scroll to the SSH Server Key Management section. A page similar to the one in the following illustration is displayed.



4. Click **Generate SSH Server Private Key**. A progress window is displayed. Wait for the operation to finish. This step might take several minutes to complete.

Enabling the secure shell server

From the Security page you can enable or disable the secure shell server. The selection that you make takes effect only after the management module is restarted. The value displayed on the screen (Enabled or Disabled) is the last value selected and is the value used when the management module is restarted.

Note: You can enable the secure shell server only if a valid secure shell server private key is installed.

Complete the following steps to enable the secure shell server:

1. In the navigation pane, click **Security**.

2. Scroll to the Secure Shell (SSH) Server section. A page similar to the one in the following illustration is displayed.

3. Click **Enabled** in the **SSH Server** field.
4. In the navigation pane, click **Restart ASM** to restart the management module.

Using the secure shell server

If you are using the secure shell client that is included in Red Hat Linux version 7.3, to start a secure shell session to a management module with network address 192.168.70.2, type a command similar to the following example:

```
ssh -x -l USERID 192.168.70.2
```

where *-x* indicates no X Window System forwarding and *-l* indicates that the session should use the user ID 'USERID'.

Using the configuration file

Use the management-module Web interface **MM Control → Configuration File** to:

- Back up the management-module configuration
- Restore the management-module configuration

Note: If you cannot communicate with a replacement management module through the Web interface or the IBM Director programs, the IP address might be different from the IP address of the management module just removed. Press the IP reset button to set the management module to the factory default IP addresses; then, access the management module using the factory IP address (see "Configuring the management module for remote access" on page 8 for the factory IP addresses) and configure the management module or load the saved configuration file.

Backing up your current configuration

You can download a copy of your current management-module configuration to the client computer that is running the management-module Web interface. Use this backup copy to restore your management-module configuration if it is accidentally

changed or damaged. Use it as a base that you can modify to configure multiple management modules with similar configurations.

Complete the following steps to back up your current configuration:

1. Log in to the management module where you want to back up your current configuration. For more information, see “Starting the management-module Web interface” on page 12.
2. In the navigation pane, click **MM Control → Configuration File**.
3. In the **Backup MM Configuration** section, click **view the current configuration summary**.

   Note: The security settings on the **Security** page are not backed up.
4. Verify the settings and then click **Close**.
5. To back up this configuration, click **Backup**.
6. Type a name for the backup, select the location where the file will be saved, and then click **Save**.
   - In Netscape Navigator, click **Save File**.
   - In Microsoft Internet Explorer, select **Save this file to disk**, and then click **OK**.

Restoring and modifying your ASM configuration

You can restore a saved configuration in full, or you can modify key fields in the saved configuration before restoring the configuration to your management module. Modifying the configuration file before restoring it helps you set up multiple management modules with similar configurations. You can quickly specify parameters that require unique values such as names and IP addresses, without having to enter common, shared information.

Complete the following steps to restore or modify your current configuration:

1. Log in to the management module where you want to restore the configuration. For more information, see “Starting the management-module Web interface” on page 12.
2. In the navigation pane, click **MM Control → Configuration File**.
3. In the **Restore MM Configuration** section, click **Browse**.
4. Click the configuration file that you want; then, click **Open**. The file (including the full path) appears in the box beside **Browse**.
5. If you do not want to make changes to the configuration file, click **Restore**. A new window opens with the management-module configuration information. Verify that this is the configuration that you want to restore. If it is not the correct configuration, click **Cancel**.

   If you want to make changes to the configuration file before restoring, click **Modify and Restore** to open an editable configuration summary window. Initially, only the fields that allow changes appear. To change between this view and the complete configuration summary view, click the **Toggle View** button at the top or bottom of the window. To modify the contents of a field, click the corresponding text box and enter the data.

   Note: When you click **Restore** or **Modify and Restore**, an alert window might open if the configuration file you are attempting to restore was created by a management module with older firmware (and therefore, less functionality). This alert message will include a list of

system-management functions that you will have to configure manually after the restoration is complete. Some functions require configurations on more than one window.

6. To proceed with restoring this file to the management module, click **Restore Configuration**. A progress indicator appears as the firmware on the management module is updated. A confirmation window opens to verify whether the update was successful.

   Note: The security settings on the **Security** page are not restored with the restore operation. To modify security settings, see “Secure Web server and secure LDAP” on page 42.

7. After receiving a confirmation that the restore process is complete, in the navigation pane, click **MM Control → Restart MM**; then, click **Restart**.
8. Click **OK** to confirm that you want to restart your management module.
9. Click **OK** to close the current browser window.
10. To log in to the management module again, start your browser, and follow your regular login process.

Appendix A. 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 BladeCenter, xSeries®, or IntelliStation® system, and whom to call for service, if it is necessary.

Before you call

Before you call, make sure that you have taken these steps to try to solve the problem yourself:

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system is turned on.
- Use the troubleshooting information in your system documentation, and use the diagnostic tools that come with your system. Information about diagnostic tools is in the *Hardware Maintenance Manual and Troubleshooting Guide* on the IBM *xSeries Documentation* CD or in the IntelliStation *Hardware Maintenance Manual* at the IBM Support Web site.
- Go to the IBM Support Web site at http://www.ibm.com/pc/support/ to check for technical information, hints, tips, and new device drivers or to submit a request for information.

You can solve many problems without outside assistance by following the troubleshooting procedures that IBM provides in the online help or in the publications that are provided with your system and software. The information that comes with your system also describes the diagnostic tests that you can perform. Most xSeries and IntelliStation systems, operating systems, and programs come with information that contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the information for the operating system or program.

Using the documentation

Information about your IBM xSeries or IntelliStation system and preinstalled software, if any, is available in the documentation that comes with your system. That documentation includes printed books, online books, readme files, and help files. See the troubleshooting information in your system documentation for instructions for using the diagnostic programs. The troubleshooting information or the diagnostic programs might tell you that you need additional or updated device drivers or other software. IBM maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. To access these pages, go to http://www.ibm.com/pc/support/ and follow the instructions. Also, you can order publications through the IBM Publications Ordering System at
http://www.elink.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/.

Software service and support

Through IBM Support Line, you can get telephone assistance, for a fee, with usage, configuration, and software problems with xSeries servers, IntelliStation workstations, and appliances. For information about which products are supported by Support Line in your country or region, go to http://www.ibm.com/services/sl/products/.

For more information about Support Line and other IBM services, go to http://www.ibm.com/services/, or go to http://www.ibm.com/planetwide/ for support telephone numbers. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

Hardware service and support

You can receive hardware service through IBM Integrated Technology Services or through your IBM reseller, if your reseller is authorized by IBM to provide warranty service. Go to http://www.ibm.com/planetwide/ for support telephone numbers, or in the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

In the U.S. and Canada, hardware service and support is available 24 hours a day, 7 days a week. In the U.K., these services are available Monday through Friday, from 9 a.m. to 6 p.m.

Appendix B. Notices

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

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

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

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

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

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

Edition notice

Trademarks

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

Active Memory	Predictive Failure Analysis
Active PCI	PS/2
Active PCI-X	ServeRAID
Alert on LAN	ServerGuide
BladeCenter	ServerProven
C2T Interconnect	TechConnect
Chipkill	ThinkPad
EtherJet	Tivoli
e-business logo	Tivoli Enterprise
@server	Update Connector
FlashCopy	Wake on LAN
IBM	XA-32
IBM (logo)	XA-64
IntelliStation	X-Architecture
NetBAY	XceL4
Netfinity	XpandOnDemand
NetView	xSeries
OS/2 WARP	

Lotus, Lotus Notes, SmartSuite, and Domino are trademarks of Lotus Development Corporation and/or IBM Corporation in the United States, other countries, or both.

Intel, MMX, and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

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

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

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

Important notes

Processor speeds indicate the internal clock speed of the microprocessor; other factors also affect application performance.

CD-ROM drive speeds list the variable read rate. Actual speeds vary and are often less than the maximum possible.

When referring to processor storage, real and virtual storage, or channel volume, KB stands for approximately 1000 bytes, MB stands for approximately 1 000 000 bytes, and GB stands for approximately 1 000 000 000 bytes.

When referring to hard disk drive capacity or communications volume, MB stands for 1 000 000 bytes, and GB stands for 1 000 000 000 bytes. Total user-accessible capacity may vary depending on operating environments.

Maximum internal hard disk drive capacities assume the replacement of any standard hard disk drives and population of all hard disk drive bays with the largest currently supported drives available from IBM.

Maximum memory may require replacement of the standard memory with an optional memory module.

IBM makes no representation or warranties regarding non-IBM products and services that are ServerProven®, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. These products are offered and warranted solely by third parties.

IBM makes no representations or warranties with respect to non-IBM products. Support (if any) for the non-IBM products is provided by the third party, not IBM.

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

Product recycling and disposal

This unit contains materials such as circuit boards, cables, electromagnetic compatibility gaskets, and connectors which may contain lead and copper/beryllium alloys that require special handling and disposal at end of life. Before this unit is disposed of, these materials must be removed and recycled or discarded according to applicable regulations. IBM offers product-return programs in several countries. Information on product recycling offerings can be found on IBM's Internet site at http://www.ibm.com/ibm/environment/products/prp.shtml.

Electronic emission notices

Federal Communications Commission (FCC) statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada Class A emission compliance statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Australia and New Zealand Class A statement

Attention: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

United Kingdom telecommunications safety requirement

Notice to Customers

This apparatus is approved under approval number NS/G/1234/J/100003 for indirect connection to public telecommunication systems in the United Kingdom.

European Union EMC Directive conformance statement

This product is in conformity with the protection requirements of EU Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a nonrecommended modification of the product, including the fitting of non-IBM option cards.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to CISPR 22/European Standard EN 55022. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

Attention: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Taiwanese Class A warning statement

警告使用者:
這是甲類的資訊產品，在
居住的環境中使用時，可
能會造成射頻干擾，在這
種情況下，使用者會被要
求採取某些適當的對策。

Chinese Class A warning statement

声　　明
此为 A 级产品。在生活环境中，
该产品可能会造成无线电干扰。
在这种情况下，可能需要用户对其
干扰采取切实可行的措施。

Japanese Voluntary Control Council for Interference (VCCI) statement

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Index

N

P

R

S

T

U

V

W

Part Number: 13N0318

Printed in USA

(1P) P/N: 13N0318