

BladeCenter Management Module  
BladeCenter T Management Module



# User's Guide



BladeCenter Management Module  
BladeCenter T Management Module



# User's Guide

**Note:** Before using this information and the product it supports, read the general information in Appendix A, "Getting help and technical assistance," on page 91 and Appendix B, "Notices," on page 93.

**Seventeenth Edition (November 2008)**

**© Copyright IBM Corporation 2008.**

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

---

# Contents

## Chapter 1. The BladeCenter management module . . . . . 1

- Accessibility features for the BladeCenter management module . . . . . 2
- Related documentation . . . . . 2
- Notices and statements in this documentation . . . 3

## Chapter 2. Using the management-module Web interface. . . 5

- Connecting to the management module . . . . . 5
  - Management-module connection overview . . . 6
  - Cabling the management module . . . . . 7
  - Connecting to the management module for the first time. . . . . 8
- Starting the management-module Web interface . . 8
- Configuring the management module . . . . . 10
  - Configuring the management module for remote access . . . . . 11
  - Configuring the management-module Ethernet ports . . . . . 12
- Communicating with the IBM Director software . . 13
- Configuring advanced features . . . . . 14
  - Network and security configuration . . . . . 15
  - Configuring Wake on LAN . . . . . 40
  - Using the configuration file . . . . . 42
  - Using the remote disk feature . . . . . 44
- Configuring an I/O module . . . . . 46

## Chapter 3. Management-module Web interface overview . . . . . 49

- Web interface pages and user roles . . . . . 49
- Management-module Web interface options . . . 52
  - Monitors . . . . . 52
  - Blade Tasks . . . . . 66
  - I/O Module Tasks . . . . . 73
  - MM Control . . . . . 77

## Appendix A. Getting help and technical assistance . . . . . 91

- Before you call . . . . . 91
- Using the documentation . . . . . 91
- Getting help and information from the World Wide Web . . . . . 92
- Software service and support . . . . . 92
- Hardware service and support . . . . . 92
- IBM Taiwan product service . . . . . 92

## Appendix B. Notices . . . . . 93

- Trademarks . . . . . 93
- Important notes . . . . . 94

## Index . . . . . 97



---

## Chapter 1. The BladeCenter management module

This *Management Module User's Guide* contains information about configuring the management module and managing components that are installed in an IBM® BladeCenter unit. Information about configuring the advanced management module is in a separate document.

**Note:** See “Starting the management-module Web interface” on page 8 for information about how you can determine which type of management module you are using.

Although all types of management module have similar function, their physical attributes might vary. See the *Installation Guide* for your management module for information about management-module controls and indicators, installation, cabling, and configuration.

All IBM BladeCenter units are referred to throughout this document as the BladeCenter unit. All management modules are referred to throughout this document as the management module. Unless otherwise noted, all commands can be run on all management-module and BladeCenter unit types.

The management module provides systems-management functions and keyboard/video/mouse (KVM) multiplexing for all of the blade servers in the BladeCenter unit that support KVM. It controls the external keyboard, mouse, and video connections, for use by a local console, and a 10/100 Mbps Ethernet remote management connection.

Each BladeCenter unit comes with at least one management module. Some BladeCenter units support installation of a second, standby management module. Only one of the management modules in a BladeCenter unit can control the BladeCenter unit at any one time, and this management module functions as the primary management module. If a standby management module is installed, it does not control the BladeCenter unit until it is switched to act as primary, either manually or automatically, if the primary management module fails.

If two management modules are installed in a BladeCenter unit, they must be of the same type: the advanced management module is not compatible for installation in the same BladeCenter unit with other management-module types. Before control can switch between the primary and standby management modules, both management modules must have the same level of firmware and, in some cases, the same IP address. The firmware level must support redundant management-module function, to enable changeover of control from the primary (active) management module to the standby management module. The latest level of management-module firmware is available at <http://www.ibm.com/systems/support/>.

**Note:** After failover, you might not be able to establish a network connection to the management module for 5 minutes.

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 (removable-media drives and USB ports).

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

**Note:** The sample screens and pages in this document might differ slightly from the screens and pages that your system displays. Content varies according to the type of BladeCenter unit that you are using and the firmware versions and optional devices that are installed.

---

## Accessibility features for the BladeCenter management module

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully.

### Accessibility features

Accessibility for the BladeCenter management module interface is provided through the command-line interface. The remote control video feed is not accessible to a screen reader.

The BladeCenter Information Center is accessibility-enabled. The accessibility features of the information center include:

- Keyboard-only operation
- Interfaces that are commonly used by screen readers. (The Java access bridge must be installed to make Java applets available to the JAWS screen reader.)
- The attachment of alternative input and output devices

### Keyboard navigation

This product uses standard Microsoft® Windows® navigation keys.

### Related accessibility information

You can view the publications for IBM BladeCenter in Adobe® Portable Document Format (PDF) using the Adobe Acrobat® Reader. The PDFs are provided on a CD that is packaged with the product, or you can access them through the IBM BladeCenter Information Center.

### IBM and accessibility

See the IBM Human Ability and Accessibility Center for more information about the commitment that IBM has to accessibility.

---

## Related documentation

Related documentation for the *BladeCenter Management Module User's Guide* is available on the Documentation CD and at <http://www.ibm.com/systems/support/>.

In addition to this *User's Guide*, the following documentation might be on the *Documentation CD* that comes with your BladeCenter management module, in Portable Document Format (PDF). Depending on your BladeCenter product, additional documents might also be included on the *Documentation CD*. The most recent versions of all BladeCenter documentation are at <http://www.ibm.com/systems/support/>.

- *Safety Information*

This document contains translated caution and danger statements. Each caution and danger statement in the documentation has a number that you can use to locate the corresponding statement in your language in the *Safety Information* document.

- *Management Module Installation Guide*

Each management module has a customized *Installation Guide* that contains instructions for installing the management module in a BladeCenter unit and creating the initial configuration. This document also contains safety and warranty information that is specific to the management module.

- *BladeCenter Management Module Command-Line Interface Reference Guide*

This document explains how to use the management-module command-line interface to directly access BladeCenter management functions as an alternative to using the Web-based user interface. The command-line interface also provides access to the text-console command prompt on each blade server through a Serial over LAN (SOL) connection.

- *IBM BladeCenter Serial over LAN Setup Guide*

This document explains how to update and configure BladeCenter components for Serial over LAN (SOL) operation. The SOL connection provides access to the text-console command prompt on each blade server and enables the blade servers to be managed from a remote location.

In addition to the documentation in this library, be sure to review the *IBM BladeCenter Planning and Installation Guide* for your BladeCenter unit for information to help you prepare for system installation and configuration. This document is available at <http://www.ibm.com/systems/support/>.

---

## Notices and statements in this documentation

A number of notices and statements are used in the documentation.

The caution and danger statements in this documentation are also in the multilingual *Safety Information* document, which is on the *IBM BladeCenter Documentation CD*. Each statement is numbered for reference to the corresponding statement in the *Safety Information* document.

The following notices and statements are used in this documentation:

- **Note:** These notices provide important tips, guidance, or advice.
- **Important:** These notices provide information or advice that might help you avoid inconvenient or problem situations.
- **Attention:** These notices indicate possible damage to programs, devices, or data. An attention notice is placed just before the instruction or situation in which damage might occur.
- **Caution:** These statements indicate situations that can be potentially hazardous to you. A caution statement is placed just before the description of a potentially hazardous procedure step or situation.

- **Danger:** These statements indicate situations that can be potentially lethal or extremely hazardous to you. A danger statement is placed just before the description of a potentially lethal or extremely hazardous procedure step or situation.

---

## Chapter 2. Using the management-module Web interface

See the following topics for instructions for using the management-module Web interface:

- “Connecting to the management module”
- “Starting the management-module Web interface” on page 8
- “Configuring the management module” on page 10
- “Communicating with the IBM Director software” on page 13
- “Configuring advanced features” on page 14
- “Configuring an I/O module” on page 46

See Chapter 3, “Management-module Web interface overview,” on page 49 for a detailed description of the structure and content of the management-module Web interface. You can also perform Web interface functions through the management-module command-line interface (CLI). See the *BladeCenter Management Module Command-Line Interface Reference Guide* for information and instructions.

---

### Connecting to the management module

You can access and manage the management module by using a specified Web browser.

A remote console connection to the management module is required to configure and manage operation of the BladeCenter unit. All management-module types support connection through the remote management and console (Ethernet) connector.

You can manage the BladeCenter unit and blade servers that support KVM by using the graphical user interface that is provided by the management-module Web interface or by using the command-line interface that you access through Telnet. All management connections to blade servers that do not support KVM are made through the management-module command-line (text only) interface.

You can perform initial configuration of the management module after you connect it to your network; however, because of some requirements that are imposed by the default management-module settings, it might be easier to perform these setup operations by using a temporary connection. The following information is in this section:

- “Management-module connection overview” on page 6
- “Cabling the management module” on page 7
- “Connecting to the management module for the first time” on page 8

After you complete the initial cabling and configuration, you can navigate to the management module by using a standard Web browser. Go to “Starting the management-module Web interface” on page 8 for more information.

## Management-module connection overview

You can access the management-module Web interface through a network or through a computer that is connected directly to the management module.

To connect a remote console to the management-module Web interface, you need the following equipment and information:

- A computer with Internet browser capability. To facilitate connections at multiple locations, you can use a notebook computer.
- The management-module MAC address that is listed on the label on the management module, if you need to look up the management-module IP address on a DHCP server.
- For a networked connection to the management module, the following equipment:
  - A standard Ethernet cable
  - A local Ethernet network port (facility connection)
- For direct connection of a computer to the management module remote management and console (Ethernet) connector, an Ethernet crossover cable.

### Hardware requirements

The client computer must have, at minimum, the following performance level in order to use the Remote Control feature that provides KVM access to a blade server:

- Intel Pentium III or later, operating at 700 MHz or faster (or equivalent)
- Memory: 256 MB RAM
- Video: 16MB RADEON 7500 ATI Mobility video chip set or equivalent (AGP 4X with 16 MB of video memory)

The following table lists the only blade server specified video resolution and refresh rate combinations, for KVM equipped blade servers, that are supported for all system configurations. Unless noted otherwise, these settings apply to all management-module types.

Resolution	Refresh rate
640 x 480	60 Hz
640 x 480	72 Hz
640 x 480	75 Hz
640 x 480	85 Hz
800 x 600	60 Hz
800 x 600	72 Hz
800 x 600	75 Hz
800 x 600	85 Hz
1024 x 768	60 Hz
1024 x 768	75 Hz

### Software requirements

The management module supports the following Web browsers for remote (client) access:

- Microsoft Internet Explorer 5.5 or later (with the latest Service Pack installed)
- Mozilla Firefox version 1.07 or later

The client Web browser that you use must be Java™-enabled, must support JavaScript version 1.2 or later, and must have the Java Virtual Machine (JVM) Plug-in version 1.4.2\_08 or later, but earlier than 1.6.0 (JRE 6.0) installed. The JVM Plug-in is available at <http://www.java.com/>.

The following server operating systems have USB support, which is required for the Remote Control feature:

- Microsoft Windows Server 2003
- Microsoft Windows 2000 with Service Pack 4 or later
- Red Hat Enterprise Linux Version 3, update 8
- SUSE Enterprise Linux version 9
- VMware version 3.0.1

The management-module Web interface does not support the double-byte character set (DBCS) languages.

## Cabling the management module

You can connect the management module to a network or directly to a client computer.

See the *Installation Guide* for your management module for specific cabling instructions. See the *BladeCenter Management Module Command-Line Interface Reference Guide* for information about connecting a remote console to the management module and using the management-module CLI to configure the BladeCenter unit.

After you cable the management module for initial configuration, see “Connecting to the management module for the first time” on page 8. See the *Installation Guide* for your management module for specific cabling information.

### Networked connection

Use an Ethernet cable to connect the management module to a network.

Connect one end of a Category 5 or higher Ethernet cable to the remote management and console (Ethernet) connector of the management module. Connect the other end of the Ethernet cable to the facility network.

### Direct connection

Use an Ethernet cable to connect a client computer directly to the management module.

Connect one end of a Category 5 or higher Ethernet crossover cable to the remote management and console (Ethernet) connector of the management module. Connect the other end of the cable to the Ethernet connector on the client computer.

## Connecting to the management module for the first time

Connect a remote console to the management module to perform initial configuration of the BladeCenter unit.

The management module has the following default network settings:

- IP address: 192.168.70.125 (primary and secondary management module)
- Subnet: 255.255.255.0
- User ID: USERID (all capital letters)
- Password: PASSWORD (note the number zero, not the letter O, in PASSWORD)

By default, the management module is configured to respond to DHCP first before it uses its static IP address.

The client computer that you connect to the management module must be configured to operate on the same subnet as the BladeCenter management module. The IP address of the management module must also be in the same local domain as the client computer. To connect a client computer to the management module for the first time, you must change the Internet protocol properties on the client computer.

After you connect the Ethernet cable from the management module to the client computer, complete the following steps:

1. Make sure that the subnet of the client computer is set to the same value as the default management module subnet (255.255.255.0).
2. Open a Web browser on the client computer, and direct it to the default management-module IP address (192.168.70.125).
3. Enter the default user name, USERID, and the default password, PASSWORD, to start the remote session.
4. Follow the instructions on the screen. Be sure to set the timeout value that you want for your Web session.

After you connect a client computer to the management module for the first time, perform the initial configuration of the BladeCenter unit (see “Configuring the management module” on page 10).

---

## Starting the management-module Web interface

Use a specified Web browser to start a Web interface session with the management module.

The management module supports the following Web browsers for remote (client) access:

- Microsoft Internet Explorer 5.5 or later (with the latest Service Pack installed)
- Mozilla Firefox version 1.07 or later

To start the management-module Web interface, complete the following steps:

1. Open a Web browser. In the address or URL field, type the IP address or host name that is defined for the management-module remote connection (see the *Installation Guide* for your management module for details).

The Enter Network Password page 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 as follows:

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

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

The BladeCenter management-module Web-interface page opens. The content of this and all other Web-interface pages varies according to the type of BladeCenter unit that you are using and the firmware versions and options that are installed. See Chapter 3, “Management-module Web interface overview,” on page 49 for detailed information about the management-module Web interface.

The following illustration shows a management-module Web-interface page.

**System Status Summary**

System is operating normally. All monitored parameters are OK.

The following links can be used to view the status of different components.

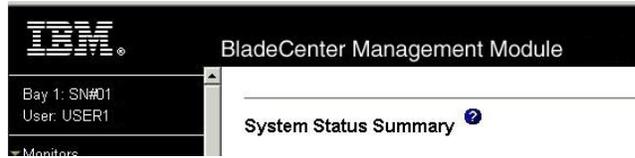
- [Blade Servers](#)
- [I/O Modules](#)
- [Management Modules](#)
- [Power Modules](#)
- [Blowers](#)
- [Front Panel](#)

**Blade Servers**

Click the icon in the Status column to view detailed information about each blade server.

Bay	Status	Name	Pwr	Owner**		Network		WOL*	Local Control			BEM*
				KVM	MT*	Onboard	Card		Pwr	KVM	MT*	
1	●	SN#J1RNE34911N	On	X	X	Eth	---   ---   ---	On	X	X	X	
2	●	SN#ZJ1WLW47T16N	On			Eth	---   ---   ---	On	X	X	X	
3	●	SN#ZJ1WS447L14E	Off			Eth	Eth   ---   ---	On	X	X	X	
4	●	McCarran	Off			Eth	---   ---   ---	On	X	X	X	
6		No blade present										
7		No blade present										
8		No blade present										
9		No blade present										
10		No blade present										
11		No blade present										

The top of the management-module Web-interface page shows the type of management module that you are logged in to. The following illustrations show the management-module types for a management module and advanced management module. Information about configuring the advanced management module is in a separate document.



The top of the management-module Web-interface page shows the login ID of the current user and the location and identity of the active (primary) management module. In the first example for a management module other than an advanced management module, the upper-left corner of the page shows a login ID of USER1 and that the primary management module, identified as SN#01, installed in management-module bay 1. In the second example for an advanced management module, the top center of the page shows a login ID of USERID and upper-left corner of the page shows that the primary advanced management module, identified as SN#YK11826B61CL, is installed in management-module bay 1.

---

## Configuring the management module

You configure the primary (active) management module; the standby management module, if present, automatically synchronizes its configuration to match that of the primary management module. This synchronization can take up to 45 minutes.

The configuration information in this documentation applies to the primary management module, which might be the only management module in the BladeCenter unit.

If the management module that you installed is a replacement for the only management module in the BladeCenter unit and you saved the configuration file before you replaced the management module, you can apply the saved configuration file to the replacement management module by using the management-module Web interface. See “Restoring and modifying your management-module configuration” on page 43 for information about applying a saved configuration file.

The BladeCenter unit automatically detects the modules and blade servers that are installed and stores the vital product data (VPD). When the BladeCenter unit is started, the management module automatically configures the remote management port of the management module so that you can configure and manage BladeCenter components. You configure and manage BladeCenter components remotely by using the management-module Web interface, the management-module command-line interface (CLI), or simple network management protocol (SNMP).

**Note:** There are two ways to configure the I/O modules: through the management-module Web interface or through an external I/O-module port that is enabled through the management module through a Telnet interface or a Web browser. See the documentation that comes with each I/O module for information.

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

- The external Ethernet (remote management) port (Ethernet 0) of the management module (see “Network Interfaces” on page 85). The initial automatic management-module configuration 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 internal Ethernet port (Ethernet 1) on the management module for communication with the I/O modules (see “Network Interfaces” on page 85).
- The management port on each I/O module which provides for communication with the management module. You configure this port by configuring the IP address for the I/O module (see “Configuration” on page 75).

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

See the documentation that comes with each I/O module to determine what else you must configure in the I/O module.

To communicate with the blade servers for functions such as deploying an operating system or application program over a network, you must also configure at least one external (in-band) port on an Ethernet switch module in I/O-module bay 1 or 2.

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

## Configuring the management module for remote access

You can configure the management module to use Dynamic Host Configuration Protocol (DHCP) or static IP addresses 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, IP address, gateway address, subnet mask, and DNS server IP address are set automatically. The host name is set to the management-module MAC address by default, and the domain server cannot change it.
- 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.

**Important:** You cannot connect to the management module using the factory-defined static IP address and default subnet address until after this period passes.

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

Make sure that the client 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 8 for more information). In the browser Address or URL field, specify the IP address that 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 MMxxxxxxxxxxx, 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.

## Configuring the management-module Ethernet ports

You can use the Web interface to configure the management-module internal and external Ethernet ports and the internal Ethernet management port on each I/O module.

To configure the management-module internal and external Ethernet ports, complete the following steps:

1. Under **MM Control** in the navigation pane, click **Network Interfaces**.
2. Configure the two Ethernet interfaces: external (remote management and console), and internal (communication with the I/O modules).

**Note:** For I/O-module communication with a remote management station, such as a management server that is running 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.
  - **Interface:** Select **Enabled** (the default) to use the Ethernet connection.
  - **DHCP:** Select one of the following choices:
    - **Enabled - Obtain IP config. from DHCP server**
    - **Disabled - Use static IP configuration**
    - **Try DHCP server. If it fails, use static IP config.** (the default, DHCP times out after 2 minutes).
  - **Hostname:** (Optional) This is the IP host name that you want to use for the management module (maximum of 63 characters and following host-naming standards).
  - **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 through 255, separated by periods, with no spaces or consecutive periods. The default setting is 192.168.70.125.

- **Subnet mask:** Four integers from 0 through 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 through 255, separated by periods, with no spaces. This address must be accessible from the IP address and subnet mask.
  - **Internal Network Interface (eth1)** - This interface communicates with the I/O modules.
    - 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.
3. Configure the internal Ethernet management port on each I/O module in the BladeCenter unit.

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

- a. Under **I/O Module Tasks** in the navigation pane, click **Configuration**.
- b. Click **Bay 1**.
- c. In the **New Static IP address** fields, specify the IP configuration to use for this interface. The subnet mask must be the same as the subnet mask in the internal network interface (eth1).
- d. Click **Advanced Configuration**.
- e. In the **Advanced Setup** section, enable external management over all ports.
- f. Under **I/O Module Tasks** in the navigation pane, click **Admin/Power/Restart**.
- g. In the **I/O Module Advanced Setup** section, select I/O module 1; then, enable the external ports. (External ports have a default value of Disabled.)

**Note:** The initial user ID and password for the I/O module firmware are as follows:

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

Repeat step 3 for each I/O module in the BladeCenter unit.

To communicate with the blade servers for functions such as deploying an operating system or application program, you also must configure at least one external (in-band) port on an Ethernet I/O module.

---

## Communicating with the IBM Director software

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

See [http://www.ibm.com/servers/eserver/xseries/systems\\_management/xseries\\_sm/dwnl.html](http://www.ibm.com/servers/eserver/xseries/systems_management/xseries_sm/dwnl.html) for the version of IBM Director software that you can use to manage redundant management modules.

For you to configure the remote alert recipients for IBM Director over LAN, the remote alert recipient must be an IBM Director-enabled server.

To communicate with the BladeCenter unit, the IBM Director software needs a managed object (in the Group Contents page 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, after 2 minutes the management module uses the static IP address that is assigned to it. Therefore, the DHCP server (if it is 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 you attempt 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 a remote management station, such as a management server that is running 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.

---

## Configuring advanced features

The following topics provide instructions for performing some of the functions that the management-module Web interface supports.

- “Network and security configuration” on page 15
- “Configuring Wake on LAN” on page 40
- “Using the configuration file” on page 42
- “Using the remote disk feature” on page 44

Detailed descriptions of the management-module Web interface are in Chapter 3, “Management-module Web interface overview,” on page 49.

## Network and security configuration

The following topics describe how to configure management-module networking and security parameters for several standard protocols.

- SNMP and DNS (see “Configuring SNMP”)
- SMTP (see “Configuring SMTP” on page 18)
- SSL and LDAP (see “Configuring LDAP” on page 19)
- Secure Web server and secure LDAP (see “Secure Web server and secure LDAP” on page 28)
- SSH (see “Configuring the Secure Shell (SSH) server” on page 38)

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

To configure SNMP, complete the following steps:

1. Log in to the management module on which you want to configure SNMP. For more information, see “Starting the management-module Web interface” on page 8
2. In the navigation pane, click **MM Control** → **General Settings**. In the management-module information page that opens, specify the following information:
  - **Name:** The name that you want to use to identify the management module. The name is included with email and SNMP alert notifications to identify the source of the alert. If more than one management module is installed in a BladeCenter unit, each management module can be given a unique name.
  - **Contact:** The name and phone number of the person to contact if there is a problem with the BladeCenter unit.
  - **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.

---

## Simple Network Management Protocol (SNMP)

SNMPv1 agent   
SNMPv3 agent   
SNMP traps

### SNMPv1 Communities

Community Name	Access Type	Host Name or IP Address
<input type="text" value="public"/>	<input type="text" value="Get"/>	1. <input type="text" value="0.0.0.0"/> 2. <input type="text"/> 3. <input type="text"/>
<input type="text" value="private"/>	<input type="text" value="Set"/>	1. <input type="text" value="0.0.0.0"/> 2. <input type="text"/> 3. <input type="text"/>
<input type="text"/>	<input type="text" value="Get"/>	1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/>

### SNMPv3 Users

If you enabled the SNMPv3 agent, you must configure SNMPv3 settings for active login profiles in order for the interaction between the SNMPv3 manager and SNMPv3 agent to work properly. You can configure these settings at the bottom of the individual login profile pages which can be reached via the [Login Profiles](#) page. Click the link for the login profile to configure, scroll to the bottom of the page and then click the "Configure SNMPv3 User" link.

5. Select **Enabled** in the applicable SNMP agent fields and in the **SNMP traps** field to forward alerts to SNMP communities and users on your network. For you to enable an 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.
  - For SNMPv1, at least one community name must be specified, with an access type set for each community name:
    - **Get:** All hosts in the community can query MIB objects and receive traps.
    - **Set:** All hosts in the community can query and set MIB objects and receive traps.
    - **Trap:** All hosts in the community can receive traps.
  - At least one valid IP address or host name (if DNS is enabled) must be specified for each community.
  - For SNMPv3, each SNMPv3 user must be configured.

**Note:** Alert recipients whose notification method is SNMP will not receive alerts unless both the SNMP agent and the SNMP traps are enabled.

6. If you are enabling the SNMPv1 agent, complete the following steps to set up a community that defines the administrative relationship between SNMP agents and SNMP managers; otherwise, continue with step 7 on page 17. You must define at least one SNMPv1 community. Each community definition consists of the following parameters:
  - Community name
  - Host name or IP address

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

### Notes:

- If an error message window opens, make the necessary adjustments to the fields that are listed in the error window; then, scroll to the bottom of the

page and click **Save** to save the corrected information. You must configure at least one community to enable the SNMP agent.

- You can have one wildcard IP address with 0.0.0.0 in the first position of the first community, with the access type selected as SET. This community address supports GET and SET operations from any IP address. The remaining eight community addresses enable specific IP or host addresses to specify a receiver of traps.
  - a. In the **Community Name** field, enter a name or authentication string to specify the community.
  - b. Select the **Access Type** for the community.
  - c. In the corresponding **Host Name** or **IP Address** field, enter the host name or IP address of each community manager.
7. Complete one of the following, based on DNS server availability:
- If a DNS server is not available on your network, scroll to the bottom of the page and click **Save**.
  - 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.

---

#### Domain Name System (DNS) ⓘ

DNS	<input type="text" value="Enabled"/>
DNS server IP address 1	<input type="text" value="9.37.0.5"/>
DNS server IP address 2	<input type="text" value="9.37.0.6"/>
DNS server IP address 3	<input type="text" value="0.0.0.0"/>

---

8. 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.
9. (Optional) If you enabled DNS, in the **DNS server IP address** fields, specify the IP addresses of up to three DNS servers on your network. Each IP address must contain four integers from 0 through 255, separated by periods.
10. Scroll to the bottom of the page and click **Save**.
11. If you are enabling the SNMPv3 agent, complete the following steps to configure the SNMPv3 profile for each SNMPv3 user; otherwise, continue with step 12 on page 18.
- a. Click the **Login Profiles** link in the Simple Network Management Protocol (SNMP) section or, in the navigation pane, click **MM Control** → **Login Profiles**.
  - b. Select the user that is to be configured; then, click the **Configure SNMPv3 User** link at the bottom of the Login Profile page. A page similar to the one in the following illustration is displayed.

**SNMPv3 User Profile 1** ?

Context name

Authentication protocol

Privacy protocol

Privacy password

Confirm privacy password

Access type

Hostname/IP address for traps

- c. Specify the SNMPv3 configuration information for this user; then, click **Save**.

**Note:** If the security settings require passwords, the SNMPv3 Authentication Protocol cannot be set to None if the user has an Access Type of Get or Set. This means that when passwords are required, a user can receive SNMP traps only when the SNMPv3 Authentication Protocol is set to None.

- d. Repeat step 11b on page 17 and step 11c for each SNMPv3 user.
12. In the navigation pane, click **MM Control** → **Restart MM**; then, restart the management module to activate the changes.

### Configuring SMTP

You can set up a Simple Mail Transfer Protocol (SMTP) server to send email notifications of management module events.

To specify the IP address or host name of the Simple Mail Transfer Protocol (SMTP) server, complete the following steps.

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

1. Log in to the management module on which you want to configure SMTP. For more information, see “Starting the management-module Web interface” on page 8.
2. In the navigation pane, click **MM Control** → **Network Protocols**, and scroll down to the **Simple Mail Transfer Protocol (SMTP)** section.

**Simple Mail Transfer Protocol (SMTP)** ?

SMTP server host name or IP address

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

You can configure Lightweight Directory Access Protocol (LDAP) to authenticate management module users.

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) can remotely authenticate any user access through a central LDAP server. This requires LDAP client support on the management module. You also can assign authority levels according to information that is found on the LDAP server.

You also can 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 pass only group authentication if the user belongs to at least one group that is associated with the management module.

### LDAP Configuration:

You can configure LDAP for use with a management module.

Setting up LDAP requires the following actions:

- “Setting up a client to use the LDAP server”
- “Configuring the LDAP client authentication” on page 22
- “Configuring the LDAP search attributes” on page 23

*Setting up a client to use the LDAP server:*

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

1. Log in to the management module on which you want to set up the client. For more information, see “Starting the management-module Web interface” on page 8.
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.

---

## Lightweight Directory Access Protocol (LDAP) Client

### Use DNS to Find LDAP Servers

Domain Source	<input type="text" value="Extract search domain from login id"/>
Search Domain	<input type="text"/>
Service Name	<input type="text" value="ldap"/>

### Use Pre-Configured LDAP Servers

	LDAP Server Host Name or IP Address	Port
1.	<input type="text"/>	<input type="text"/>
2.	<input type="text"/>	<input type="text"/>
3.	<input type="text"/>	<input type="text"/>

### Miscellaneous Parameters

Root DN	<input type="text"/>
Group Filter	<input type="text"/>
Binding Method	<input type="text" value="w/ Login Credentials"/>

[Set DN and password only if Binding Method used is w/ Configured Credentials](#)

[Set attribute names for LDAP client search algorithm](#)

---

3. Configure the LDAP client, using the following information:
  - a. Select **Use DNS to find LDAP Servers** or **Use Pre-Configured LDAP Servers** (default). The management module contains a Version 2.0 LDAP Client that you can configure to provide user authentication through one or more LDAP servers. The LDAP servers that are used for authentication can be discovered dynamically or manually preconfigured.
  - b. If you are using DNS to find LDAP servers, configure the following settings; then, go to step 3d on page 21. When you are discovering LDAP servers dynamically, the mechanisms that are described by RFC2782 are applied to find the servers through a process called DNS SRV.

### Domain Source

The DNS SRV request that is sent to the DNS server must specify a domain name. The LDAP client determines where to get this domain name according to the option that is selected:

**Extract search domain from login id:** The LDAP client uses the domain name in the login ID. For example, if the login ID is joesmith@mycompany.com, the domain name is mycompany.com. If the domain name cannot be extracted from the login ID, the DNS SRV process fails, causing a user authentication failure.

**Use only configured search domain below:** The LDAP client uses the domain name that is set in the **Search Domain** field.

**Try login id first, then configured value:** The LDAP client first attempts to extract the domain name from the login ID. If this succeeds, this domain name is used in the DNS SRV request. If there is no domain name in the login ID, the LDAP client uses the domain name that is set in the **Search Domain** field as the domain name in the DNS SRV request. If neither of these items is configured, user authentication fails.

### Search Domain

This optional parameter is used only when a configured search domain is being used as a domain source. This parameter might be used as the domain name in the DNS SRV request, depending on how the Domain Source parameter is configured.

### Service Name

A DNS SRV request that is sent to a DNS server must also specify a service name. If this field is not set, the DNS SRV request uses a default value of ldap. Each DNS SRV request must also specify a protocol name: this value is set totcp and is not configurable.

- c. If you are using preconfigured LDAP servers, configure the **LDAP Server Host Name or IP Address** fields; then, go to step 3d. The port number for each server is optional. If the field is left blank, the default value of 389 is used for nonsecured LDAP connections. For secured connections, the default is 636. You must configure at least one LDAP server.
- d. Configure the following items for all LDAP server types:

### Root DN

This is the distinguished name for the root entry of the directory tree on the LDAP server (for example, dn=companyABC,dn=com).

### Group Filter

The **Group Filter** field is used for group authentication. It specifies the groups that the management module belongs to. If the **Group Filter** field left blank, group authentication is disabled. If group authentication is enabled, it is performed after user authentication. Specifically, an attempt is made to match at least one group in the list to a group that the user belongs to. If there is no match, the user fails authentication and is denied access. If there is at least one match, group authentication passes. All comparisons that are made during authentication are case sensitive.

The group filter is limited to 511 characters and can contain multiple group names. A colon (:) is used to delimit group names. Leading spaces and trailing spaces are ignored; all other spaces are treated as part of the group name. The asterisk "\*" wildcard character is not treated as a wildcard, because the wildcard concept has been eliminated for security. A group name can be specified as a full domain name or using only the company name portion. For example, a group with a domain name equal to cn=adminGroup,dc=mycompany,dc=com can be specified using the actual domain name or by using adminGroup. You must also configure additional authentication attributes as described in "Configuring the LDAP search attributes" on page 23.

### Binding Method

For initial binds to the LDAP server during user authentication, select one of the following options:

**Anonymous authentication:** A bind attempt is made without a client distinguished name or password. If the bind is successful, a search is requested to find an entry on the LDAP server for the user who is attempting to log in. If an entry is found, a second attempt to bind is 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.

**w/ Configured Credentials:** A bind attempt is made, using the configured client domain name and password. If the initial bind is successful, a search is performed to find an entry on the LDAP server that belongs to the user who is logging in. If necessary, a second attempt to bind is attempted, this time with the domain name that is retrieved from the user LDAP record and the password that was entered during the login process. If this fails, the user is denied access. When using a binding method of configured credentials, you must configure the credentials as described in “Configuring the LDAP client authentication.”

**w/ Login Credentials:** A bind attempt is made, using the credentials that were supplied during the login process. If the initial bind is successful, a search is performed to find an entry on the LDAP server that belongs to the user who is logging in.

Depending on the LDAP configuration that you have set, click the options to set the domain names and passwords that are used for client authentication and the LDAP client search attributes. Each of these options is described in the following sections.

*Configuring the LDAP client authentication:*

You can configure LDAP client authentication for a management module.

If the binding method is set to configured credentials, configure LDAP client authentication by completing the following steps:

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 only if Binding Method is Client Authentication**. A page similar to the one in the following illustration is displayed.

The screenshot shows a web-based configuration interface for LDAP Client Authentication. The title is "LDAP Client Authentication" with a help icon. There are three input fields: "Client DN", "Password", and "Confirm password". The "Password" and "Confirm password" fields are masked with asterisks. At the bottom right, there are three buttons: "Reset to Defaults", "Cancel", and "Save". A link "View Configuration Summary" is located at the top right of the form area.

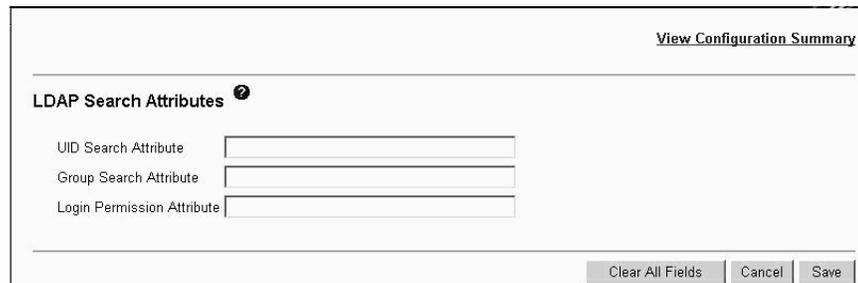
3. Perform the initial bind to the LDAP server during user authentication with anonymous authentication, client-based authentication, or user principal name. To use client-based authentication, in the **Client DN** field, type a client distinguished name. Type a password in the **Password** field or leave it blank; then, confirm it.

### Configuring the LDAP search attributes:

You can configure LDAP search attributes for a management module.

Configure the LDAP search attributes by completing the following steps:

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 attribute names for LDAP based client search algorithm**. 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 selected binding method is anonymous authentication or client authentication, the initial bind to the LDAP server is followed by a search request that is 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 that is used to represent user IDs on that server. Specifically, this name is used as a search filter against the login ID that is 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 that is used for user IDs is often sAMAccountName.

When the selected binding method 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 that is entered has the form *userid@somedomain*.

#### Group Search Attribute

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

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

#### Login Permission Attribute

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

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

- The field supports user roles for both the command authorities that are used in earlier versions of management-module firmware and the role-based user permissions for the latest version of management-module firmware. Bit positions 11 through 16 determine which type of role is used. See “Web interface pages and user roles” on page 49 for information about the commands available for each user role.
- The attribute value must be a bit string that is entered as consecutive zeros or ones, with each bit representing a particular set of functions (for example, 010000000000 or 0000110010000). The bits are numbered according to their positions. The leftmost bit is bit position 0. A value of 1 at a particular position enables the corresponding function. A value of 0 disables that function. The LDAP attribute string is copied into a local string that is 64 characters long. If fewer than 64 characters are specified, the local string is padded with zeros. If the string is longer than 64 characters, extra characters are not copied.
- The following functions are associated with the 64 bit positions:
  - User authorities (bit positions 0 through 10):
    - Deny Always (bit position 0): If this bit is set, a user will always fail authentication. This function can be used to block a particular user or users who are associated with a particular group.
    - Supervisor Access (bit position 1): If this bit is set, a user is given administrator privileges. The user has read and write access to every function. When this bit is set, other bits that define specific function access do not need to be set individually.
    - Read Only Access (bit position 2): If this bit is 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 bit position 2 having the lowest precedence. That is, if any other bit is set, this bit is ignored.
    - Networking and Security (bit position 3): If this bit is set, a user can modify the settings in the Security, Network Protocols, and Network Interface pages for MM Control. If this bit is set, a user also can modify the settings in the Management page for I/O Module Tasks.
    - User Account Management (bit position 4): If this bit is 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 this bit is set, a user can access the remote server console.
    - Blade Server Remote Console and Virtual Media Access (bit position 6): If this bit is 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 this bit is set, a user can access the power-on and restart functions for the blade servers and I/O modules.
- Basic Configuration (management module, I/O modules, blade servers) (bit position 8): If this bit is 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 this bit is set, a user can clear the event logs. Everyone can look at the event logs, but this permission is required to clear the logs.
- Advanced Configuration (management module, I/O modules, blade servers) (bit position 10): If this bit is set, a user has no restrictions when configuring the management module, blade servers, I/O modules, and VPD. The user also can 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.
- Permission version (bit positions 11 through 15): These bits specify which type of user roles, user authorities, or role-based user permissions is being used. If these bits are set to 00001, the role-based user permissions, using bits 16 through 30, are used. If these bits are set to 00000 or any other value, the user authorities, using bits 0 through 10, are used.
- Role-based user permissions (non-scripting use on all management-module types) (bit positions 16 through 30):
  - Deny Always (bit position 16): If this bit is set, a user will always fail authentication. This function can be used to block a particular user or users who are associated with a particular group.
  - Supervisor (bit position 17): If this bit is set, a user is given administrator privileges. The user has read and write access to every function. When this bit is set, other bits that define specific function access do not have to be set individually.
  - Operator (bit position 18): If this bit is set, a user can view all information. User access to information is limited by the permission scope that is specified in bits 31 through 49.
  - Chassis Operator (bit position 19): If this bit is set, a user can view information about the common BladeCenter unit components.
  - Chassis User Account Management (bit position 20): If this bit is set, a user can add, modify, and delete user login profiles. Changing the Global Login Settings requires Chassis Configuration permission.
  - Chassis Log Management (bit position 21): If this bit is set, a user can clear the event logs or change the log policy settings. All users can look at the event logs, but this permission is required to clear the logs or change the log policy settings at the top of the event-log page.
  - Chassis Configuration (bit position 22): If this bit is set, a user can perform management and setup operations for the common

BladeCenter unit components and features. User access to information is limited by the permission scope that is specified in bit 45.

- Chassis Administration (bit position 23): If this bit is set, a user can manage operation of the common BladeCenter unit components and features. User access to information is limited by the permission scope that is specified in bit 45.
- Blade Operator (bit position 24): If this bit is set, a user can view information about the blade servers. User access to blade servers is limited by the permission scope that is specified in bits 31 through 44.
- Blade Remote Presence (bit position 25): If this bit is set, a user can access the remote server console and the virtual media functions for the remote server. User access to blade servers is limited by the permission scope that is specified in bits 31 through 44.
- Blade Configuration (bit position 26): If this bit is set, a user can perform management and setup operations for the blade servers. User access to blade servers is limited by the permission scope that is specified in bits 31 through 44.
- Blade Administration (bit position 27): If this bit is set, a user can manage operation of the blade servers. User access to blade servers is limited by the permission scope that is specified in bits 31 through 44.
- Switch Operator (bit position 28): If this bit is set, a user can view information about the I/O modules. User access to I/O modules is limited by the permission scope that is specified in bits 46 through 55.
- Switch Module Configuration (bit position 29): If this bit is set, a user can perform management and setup operations for the I/O modules. User access to I/O modules is limited by the permission scope that is specified in bits 46 through 55.
- Switch Module Administration (bit position 30): If this bit is set, a user can manage operation of the I/O modules. User access to I/O modules is limited by the permission scope that is specified in bits 46 through 55.
- Permission scope (for role-based user permissions) (bit positions 31 through 55):
  - Blade 1 (bit position 31): If this bit is set, a user can access information about the blade server that is addressed in blade bay 1.
  - Blade 2 (bit position 32): If this bit is set, a user can access information about the blade server that is addressed in blade bay 2.
  - Blade 3 (bit position 33): If this bit is set, a user can access information about the blade server that is addressed in blade bay 3.
  - Blade 4 (bit position 34): If this bit is set, a user can access information about the blade server that is addressed in blade bay 4.

- Blade 5 (bit position 35): If this bit is set, a user can access information about the blade server that is addressed in blade bay 5.
- Blade 6 (bit position 36): If this bit is set, a user can access information about the blade server that is addressed in blade bay 6.
- Blade 7 (bit position 37): If this bit is set, a user can access information about the blade server that is addressed in blade bay 7.
- Blade 8 (bit position 38): If this bit is set, a user can access information about the blade server that is addressed in blade bay 8.
- Blade 9 (bit position 39): If this bit is set, a user can access information about the blade server that is addressed in blade bay 9.
- Blade 10 (bit position 40): If this bit is set, a user can access information about the blade server that is addressed in blade bay 10.
- Blade 11 (bit position 41): If this bit is set, a user can access information about the blade server that is addressed in blade bay 11.
- Blade 12 (bit position 42): If this bit is set, a user can access information about the blade server that is addressed in blade bay 12.
- Blade 13 (bit position 43): If this bit is set, a user can access information about the blade server that is addressed in blade bay 13.
- Blade 14 (bit position 44): If this bit is set, a user can access information about the blade server that is addressed in blade bay 14.
- Chassis (bit position 45): If this bit is set, a user can access information about the common BladeCenter unit components.
- I/O Module 1 (bit position 46): If this bit is set, a user can access information about the I/O module in I/O-module bay 1.
- I/O Module 2 (bit position 47): If this bit is set, a user can access information about the I/O module in I/O-module bay 2.
- I/O Module 3 (bit position 48): If this bit is set, a user can access information about the I/O module in I/O-module bay 3.
- I/O Module 4 (bit position 49): If this bit is set, a user can access information about the I/O module in I/O-module bay 4.
- I/O Module 5 (bit position 50): If this bit is set, a user can access information about the I/O module in I/O-module bay 5.
- I/O Module 6 (bit position 51): If this bit is set, a user can access information about the I/O module in I/O-module bay 6.
- I/O Module 7 (bit position 52): If this bit is set, a user can access information about the I/O module in I/O-module bay 7.
- I/O Module 8 (bit position 53): If this bit is set, a user can access information about the I/O module in I/O-module bay 8.
- I/O Module 9 (bit position 54): If this bit is set, a user can access information about the I/O module in I/O-module bay 9.

- I/O Module 10 (bit position 55): If this bit is set, a user can access information about the I/O module in I/O-module bay 10.
- Reserved (bit positions 56 through 63): These bits are reserved for future use.
- If none of the bits are set, the default is read-only for the user.
- Priority is given to login permissions that are retrieved directly from the user record. If the user record does not have the login permission attribute, an attempt is 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 is assigned the inclusive OR of all the bits for all of the groups. The Browser Only bit is set only if all the other bits are set to zero. If the Deny Always bit is set for any of the groups, the user is refused access. The Deny Always bit always has precedence over every other bit.

## Secure Web server and secure LDAP

You can set up a secure Web server and secure LDAP for the management module by using the Secure Sockets Layer (SSL).

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 1. 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 that are required for SSL.

### Configuring security:

Use the procedures 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 29.

The content of the Security Web page is context-sensitive. The selections that are 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.

Perform the following general tasks to configure the security for the management module:

1. Configure the SSL server certificates for 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 30.)
  - 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 35.)
2. Configure the SSL client certificates for secure 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 36.)
  - 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 36.)
  - 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 38.)
3. You must restart the management module to implement SSL server configuration changes (See “Restart MM” on page 89).

**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 that is signed by a certificate authority.

Using a self-signed certificate is the simplest method for using SSL, but it does create a small security risk: the SSL client has no way of validating the identity of the SSL server for the first connection that is attempted between the client and server. A third party can impersonate the server and intercept data that moves 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 is secure for that browser (assuming that the initial connection was not compromised by an attack).

For more complete security, you can use a certificate that is 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 through 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 can 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 be installed before SSL is enabled.

Two methods are available for generating the private key and required certificate: using a self-signed certificate and using a certificate that is signed by a certificate authority. To use a self-signed certificate for the SSL server, see “Generating a self-signed certificate.” To use a certificate-authority-signed certificate for the SSL server, see “Generating a certificate signing request” on page 31.

*Generating a self-signed certificate:*

To generate a new private encryption key and self-signed certificate for the management module, complete the following steps:

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

The screenshot shows a web interface for SSL configuration. It is titled "SSL Server Configuration for Web Server" and contains four main sections:

- SSL Server Configuration:** A dropdown menu is set to "Disabled" and a "Save" button is present.
- SSL Server Certificate Management:** A status message reads "SSL server certificate status: No certificate or certificate signing request (CSR) has been generated." Below this are two links: "Generate a New Key and a Self-signed Certificate" and "Generate a New Key and a Certificate Signing Request (CSR)".
- SSL Client Configuration for LDAP Client:** A dropdown menu is set to "Disabled" and a "Save" button is present.
- SSL Client Certificate Management:** A status message reads "SSL client certificate status: No certificate or certificate signing request (CSR) has been generated." Below this are two links: "Generate a New Key and a Self-signed Certificate" and "Generate a New Key and a Certificate Signing Request (CSR)".

- 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; then, click **Save**.
- 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.

---

**SSL Server Self-signed Certificate** ?

**Certificate Data**

Country (2 letter code)

State or Province

City or Locality

Organization Name

MM Host Name

**Optional Certificate Data**

Contact Person

Email Address

Organizational Unit

Surname

Given Name

Initials

DN Qualifier

- 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*. 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. It shows that a self-signed certificate is installed.

---

## SSL Server Certificate Management ?

**SSL server certificate status:** A self-signed certificate is installed.

[Generate a New Key and a Self-signed Certificate](#)

[Generate a New Key and a Certificate Signing Request \(CSR\)](#)

[Import a Signed Certificate](#)

[Download Certificate](#)

---

*Generating a certificate signing request:*

To generate a new private encryption key and certificate-signing request, complete the following steps:

- In the navigation pane, click **MM Control** → **Security**.
- 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; 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.

---

**SSL Certificate Signing Request (CSR)** 

**Certificate Request Data**

Country (2 letter code)

State or Province

City or Locality

Organization Name

MM Host Name

**Optional Certificate Data**

Contact Person

Email Address

Organizational Unit

Surname

Given Name

Initials

DN Qualifier

**CSR Attributes and Extension Attributes**

Challenge Password

Unstructured Name

---

4. Type the information in the required fields and any optional fields that apply to your configuration. The fields are the same as for a self-signed certificate, with some additional fields. The following sections describe 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 in which the management module is located. This field must contain the 2-character country code.

**State or Province**

Use this field to indicate the state or province in which the management module is located. This field can contain a maximum of 30 characters.

**City or Locality**

Use this field to indicate the city or locality in which the management module is located. This field can contain a maximum of 50 characters.

**Organization Name**

Use this field to indicate the company or organization that controls the management module. When this information is used to generate a certificate-signing request, the issuing certificate authority can verify that the organization that is 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 appears in the browser Web address field.

Make sure that the value that 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 in the certificate. To prevent certificate warnings from the browser, the value that is used in this field must match the host name that is used by the browser to connect to the management module. For example, if the Web address in the address field is `http://mm11.xyz.com/private/main.ssi`, the value that is used for the **MM Host Name** field must be `mm11.xyz.com`. If the Web address is `http://mm11/private/main.ssi`, the value that is used must be `mm11`. If the Web address is `http://192.168.70.2/private/main.ssi`, the value that is used must 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.

- **Optional certificate data**

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

#### **Contact Person**

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

#### **Email Address**

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

#### **Organizational Unit**

Use this field to indicate the unit within the company or organization that controls 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 who is 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 who is 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 who is 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.

### Years Valid

This field is present only for an SSL server; it is not shown for an SSL client.

- **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 that is assigned to the management module. This field can contain a maximum of 60 characters.

5. After you complete the information, click **Generate CSR**. The new encryption keys and CSR 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.

---

#### Download CSR

Certificate Signing Request (CSR) is ready for downloading.

To get the CSR, click "Download CSR". You can then send it to a CA for signing.

Download CSR

6. Click **Download CSR**; then, click **Save** to save the file to your computer. The file that is 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, you can convert the file by using a 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 page, PEM format is usually expected. The command for converting a certificate-signing request from DER to PEM format through OpenSSL is similar to the following command:

```
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, you might need 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 by using a tool that is provided by your certificate authority or by using a tool such as OpenSSL (<http://www.openssl.org>). The command for converting a certificate from PEM to DER format is similar to the following command

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

Go to step 8 on page 35 after the signed certificate is returned from the certificate authority.

- 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.

---

### SSL Server Certificate Management <sup>?</sup>

**SSL server certificate status:** A self-signed certificate is installed and a CSR has been generated.

[Generate a New Key and a Self-signed Certificate](#)

[Generate a New Key and a Certificate Signing Request \(CSR\)](#)

[Import a Signed Certificate](#)

[Download Certificate](#)

[Download CSR](#)

---

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

---

### Import a Signed SSL Certificate <sup>?</sup>

To import a certificate in DER format, select the file and click "Import Certificate".

---

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

### Enabling SSL for the secure Web server:

You can enable the Secure Sockets Layer (SSL) for the management-module secure Web server.

**Note:** To enable SSL, a valid SSL certificate must be installed.

To enable the secure Web server, complete the following steps:

1. In the navigation pane, click **MM Control** → **Security**. The page that is displayed is 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, see “SSL server certificate management” on page 30.



2. Scroll to the SSL Server Configuration for Web Server section and select **Enabled** in the **SSL Server** field; then, click **Save**. The selected value 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 be installed before SSL is enabled.

Two methods are available for generating the private key and required certificate: using a self-signed certificate and using a certificate that is 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. To use a self-signed certificate for the SSL client, see “Generating a self-signed certificate” on page 30. To use a certificate-authority-signed certificate for the SSL client, see “Generating a certificate signing request” on page 31.

### 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.

To import a trusted certificate, complete the following steps:

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; 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 field next to the **Browse** push 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. Continue displaying this page until the transfer is completed.

The SSL Client Trusted Certificate Management section of the **MM Control → Security** page now looks similar to the one in the following illustration.



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

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

## Enabling SSL for the LDAP client:

You can enable or disable SSL for the management module 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, you must install a valid SSL client certificate and at least one trusted certificate.

To enable SSL for the client, complete the following steps:

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

---

**SSL Client Configuration for LDAP Client** <sup>?</sup>

SSL Client

---

**SSL Server Certificate Management** <sup>?</sup>

**SSL server certificate status:** A CA-signed certificate is installed.

[Generate a New Key and a Self-signed Certificate](#)

[Generate a New Key and a Certificate Signing Request \(CSR\)](#)

---

**SSL Client Trusted Certificate Management** <sup>?</sup>

Trusted CA Certificate 1

Trusted CA Certificate 2

Trusted CA Certificate 3

---

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 selected value takes effect immediately.

## Configuring the Secure Shell (SSH) server

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

SSH users are authenticated through password authentication. For password authentication, the password is sent after the encryption channel has been established. The login ID and password pair can be one of the 12 locally stored login IDs and passwords, or they can be stored on an LDAP server.

## Generating a Secure Shell host key:

You can generate a Secure Shell host key to authenticate the identity of the Secure Shell server to the client.

The host key generation is started manually. The Secure Shell server must be disabled before you generate new Secure Shell host keys. You must manually generate the host keys before you enable the Secure Shell server.

When you request a new host key, both an RSA key and a DSA key are created to allow access to the management module. To preserve the secrecy of the private portion of the Secure Shell host key, it is not backed up during a configuration save-restore operation.

To create a new Secure Shell host key, complete the following steps:

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



4. Click **Generate SSH Server Private Key**.

The current window displays a progress page. Wait for the operation indicated by the progress page to finish. This step can take several minutes.

## Enabling the Secure Shell server:

You must manually enable SSH and manually generate an SSH host key.

The selection that you make takes effect only after the management module is restarted. The value that is displayed on the page (Enabled or Disabled) is the last selected value and is the value that is used when the management module is restarted.

**Note:** You can enable the Secure Shell server only if a valid Secure Shell host key is installed.

To enable the Secure Shell server, complete the following steps:

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.

---

## Secure Shell (SSH) Server

SSH Server	Disabled ▾
SSH version	All SSH versions ▾
	All SSH versions
	SSHv2 only

---

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:

Use the management module Secure Shell server to open a secure connection to a command-line interface.

The following SSH clients are available. Although some SSH clients have been tested, support or nonsupport of any particular SSH client is not implied.

- The SSH clients that are distributed with operating systems such as Linux, AIX®, and UNIX (see your operating-system documentation for information)
- The SSH client of cygwin (see <http://www.cygwin.com> for information)

If you are using a Secure Shell client that is based on openSSH, such as the client that is included in Red Hat Linux version 7.3, to start an interactive command-line 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 is to use the login ID `USERID`.

## Configuring Wake on LAN

You can use the management module to configure Wake on LAN for blade servers that support this feature. See the documentation for your blade server for further information.

**Note:** This feature is not available for all blade server models. See the documentation for your blade server for additional information

To configure the Wake on LAN feature in the BladeCenter unit, complete the following steps:

1. Write down the MAC address of the integrated Ethernet controllers in each blade server. You can find this information in one of the following ways. The MAC addresses are needed to configure a remote system to start the blade servers through the Wake on LAN feature: the remote system issues the Wake on LAN command (a Magic Packet frame) by sending it to a MAC address.
  - Blade server MAC addresses are part of the Vital Product Data (VPD) that the management module maintains for each installed blade server. (Go to **Monitors** → **Hardware VPD** in the management-module Web interface and view the section related to blade server hardware inventory. Click the module name of a particular blade server to access the blade server VPD data page. On this page, select the **Ports** tab at the top to view the MAC address information.
  - The MAC address is listed on the bar code label that is on the bottom of each blade server enclosure. Each blade server might also have a loose label on which the MAC addresses are printed.
  - For some blade server types, you can read the MAC address by using the blade server Configuration/Setup Utility program (**Devices and I/O Ports** → **System MAC Addresses**)
2. Make sure that the Wake on LAN feature is enabled in the BladeCenter management module (**Blade Tasks** → **Power/Restart** and **Blade Tasks** → **Configuration** in the management-module Web interface).
3. Make sure that the external ports of the Ethernet switch modules or pass-thru modules in I/O-module bays 1 and 2 are enabled (**I/O Module Tasks** → **Admin/Power/Restart** → **I/O Module Advanced Setup** in the management-module Web interface). If the external ports are not enabled, blade servers in the BladeCenter unit will not be able to communicate with the external network.

### Verifying the Wake on LAN configuration

To verify that the Wake on LAN feature was correctly configured and is functioning, complete the following steps:

1. Start the blade server operating system.
2. Attempt to ping the remote computer that will issue the Wake on LAN command (the Magic Packet frame). A successful ping verifies network connectivity.
3. Make sure that the blade server is the current owner of the keyboard, video, and mouse (KVM).
4. Shut down the blade server, insert a DOS startable (bootable) diskette into a USB attached diskette drive; then, restart the blade server.
5. When the A:\ prompt is displayed, turn off the blade server by using the power-control button.
6. Issue the Wake on LAN command (the Magic Packet frame) from the remote computer. If the Wake on LAN feature was correctly configured and is functioning, the single blade server wakes up. This is a good procedure to determine whether there is a single blade server or BladeCenter configuration problem or a device-driver problem within the operating system.

## Linux-specific configuration

To configure the Wake on LAN feature for Red Hat or SUSE Linux, complete the following steps:

1. Type the following command:  

```
insmod bcm5700.o enable_wol=1,1
```

The `enable_wol=1,1` parameter instructs the device driver to enable the Wake on LAN feature for both Broadcom controllers in a single blade server. Because there are two Broadcom controllers, you must issue a 1 for each of them.
2. Recompile the device driver for your Linux image. For example, a device driver that was compiled in Red Hat Linux is not guaranteed to function for SUSE Linux. See the documentation that comes with your operating system for information about compiling device drivers. For you to compile the Broadcom device drivers in Red Hat Linux, a default installation is not sufficient because all files that are required for a successful compilation are not included. A custom installation of Red Hat Linux, in which the packages for software and kernel development are selected, includes the files that are required for successful compilation of the device drivers.

## Using the configuration file

You can use a configuration file to back up and restore the management-module configuration.

Procedures for backing up and restoring the management-module configuration are in the following sections.

- “Backing up your management-module configuration”
- “Restoring and modifying your management-module configuration” on page 43

**Note:** If you cannot communicate with a replacement management module through the Web interface, the IP address might be different from the IP address of the management module that you removed. Use the IP reset button to set the management module to the factory default IP addresses; then, access the management module by using the factory IP address (see the *Installation Guide* for your management module for the factory IP addresses and instructions for using the IP reset button) and configure the management module or load the saved configuration file.

## Backing up your management-module configuration

Backing up the management-module configuration to a configuration file on the BladeCenter unit lets you restore your management-module configuration if it is accidentally changed or damaged.

All management-module types enable you to save your management-module configuration to a file. Backup of the management module configuration requires special user permissions (see “Web interface pages and user roles” on page 49 for information).

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.

### Backing up a management-module configuration:

You can back up the configuration of the management module.

To back up your current configuration, complete the following steps:

1. Log in to the management module for which you want to back up the current configuration. For more information, see “Starting the management-module Web interface” on page 8.
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; then, click **Close**.
5. To back up the configuration, click **Backup**.
6. Type a name for the backup, select the location where the file will be saved; then, click **Save**.
  - In Mozilla Firefox, click **Save to Disk**; then, click **OK**.
  - In Microsoft Internet Explorer, select **Save this file to disk**; then, click **OK**.

### Restoring and modifying your management-module configuration

You can restore a default or saved configuration in full, or you can modify key fields in the saved configuration before you restore the configuration to your management module.

Modifying the configuration file before you restore 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.

### Restoring a management-module configuration:

You can restore or modify your current configuration by using a saved management module configuration.

Complete the following steps:

1. Log in to the management module for which you want to restore the configuration. For more information, see “Starting the management-module Web interface” on page 8.
2. Determine the type of restoration that you want to perform: **Restore Defaults**, or **Restore Configuration from File**.
  - a. To restore the default configuration, click **MM Control → Restore Defaults** in the navigation pane; then, click **Restore Defaults**.
  - b. To restore the configuration from a file, click **MM Control → Configuration File** in the navigation pane; then, complete the following steps:
    - 1) In the **Restore MM Configuration** section, click **Browse**.
    - 2) Click the configuration file that you want; then, click **Open**. The file (including the full path) is displayed in the box next to **Browse**.
    - 3) 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 you restore it, click **Modify and Restore** to open an editable configuration summary window. Initially, only the fields that allow changes are displayed. To change between this view and the complete configuration summary, view, click **Toggle View** at the top or bottom of the window.

**Note:** When you click **Restore** or **Modify and Restore**, an alert window might open if the configuration file that you are attempting to restore was created by a management module with older firmware (and, therefore, less functionality). This alert message includes a list of systems-management functions that you must configure after the restoration is complete. Some functions require configurations on more than one window.

- 4) To proceed with restoring this file to the management module, click **Restore Configuration**. A progress indicator is displayed as the firmware on the management module is updated. A confirmation window opens to indicate 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 28

3. After you receive a confirmation that the restore process is complete, in the navigation page, click **MM Control** → **Restart MM**; then, click **Restart**.
4. Click **OK** to confirm that you want to restart the management module.
5. Click **OK** to close the browser window.
6. To log in to the management module again, start the browser, and follow your login process.

## Using the remote disk feature

The management module can use remote mass storage devices.

From the Remote Control window (see “Remote Control” on page 67), you can assign, or mount, an optical drive or diskette drive that is on the remote client computer to a blade server. By using this window, you can also specify a disk image or CD (ISO) image on the remote system for the blade server to use.

You can use the remote disk for functions such as updating blade server firmware, installing new software on the blade server, and installing or updating the operating system on the blade server. After you assign the remote disk, use the remote console function to access it. The remote disk appears as a USB drive on the blade server.

Your operating system must have USB support for you to use the remote disk feature. The following operating systems provide USB support:

- Microsoft Windows Server 2003
- Microsoft Windows 2000 with Service Pack 4 or later
- Red Hat Enterprise Linux Version 3, update 8
- SUSE Enterprise Linux version 9
- VMware version 3.0.1

In addition, the client (remote) system must have Microsoft Windows 2000 or later and must have the Java Virtual Machine (JVM) Plug-in version 1.4.2\_08 or later, but earlier than 1.6.0 (JRE 6.0). The client system must also have an Intel Pentium

III or later microprocessor operating at 700 MHz or faster (or an equivalent microprocessor).

### Mounting a disk drive or disk image

You can use the management module to mount a disk drive or disk image on a remote system to a blade server.

To mount a disk drive or disk image on a remote system to a blade server, complete the following steps:

1. Start the management-module Web interface (see “Starting the management-module Web interface” on page 8).
2. In the navigation pane, click **Blade Tasks** → **Remote Control**.
3. In the **Start Remote Control** section, click **Start Remote Control**.
4. In the **Remote Disk** section, select the resources to make available for mounting from the left side of the remote disk drive selector; then, click >> to finalize the selection and move them to the right side of the remote disk drive selector. To deselect items, select them in the right side of the remote disk drive selector; then, click <<.

You are given the option to save the disk image in the management-module random access memory (RAM) when you select a diskette drive or an image file and move it to the right side of the drive selector. A maximum of one diskette drive or drive image can be stored on the management module. The size of the drive or image contents must be 1.44 MB or less.

Saving the disk image to management module memory enables the disk image to remain mounted on the blade server so that you can access the disk image later, even if the Web interface session is terminated. Mounted drives that are not saved to the management module is unmounted when the remote-control window is closed.

**Important:** The disk image is lost when the management module is restarted or when the management-module firmware is updated. To use the mounted disk, use the remote console function. The mounted disk is displayed as a USB disk drive that is attached to the server.

5. Click **Write Protect** to prevent data from being written to the mounted drives.
6. Select from the remote disk drive selector one or more drives or images to mount; then, click **Mount Drive**. The mounted drive or disk image functions as a USB device that is connected to the blade server.

### Unmounting a disk drive or disk image

You can use the management module to unmount a disk drive or disk image from a blade server.

When you have finished using a drive or disk image, complete the following steps to close and unmount it:

1. Complete any procedures that are required by your operating system to close and unmount a remote disk or image. See the documentation for your operating system for information and instructions. For the Microsoft Windows operating system, complete one of the following procedures to close and unmount a drive or drive image:
  - If there is an unplug or eject hardware icon in the Windows taskbar, complete the following steps:
    - a. Double-click the unplug or eject hardware icon.
    - b. Select **USB Mass Storage Device** and click **Stop**.
    - c. Click **Close**.
  - If there is no unplug or eject hardware icon in the Windows taskbar, complete the following steps:
    - a. In the Microsoft Windows Control Panel, click **Add/Remove Hardware**; then, click **Next**.
    - b. Select **Uninstall/Unplug a device**; then, click **Next**.
    - c. Click **Unplug/Eject a device**; then, click **Next**.
2. In the **Remote Disk** section of the Remote Control window of the management-module Web interface, click **Unmount Drive**.

---

## Configuring an I/O module

You can configure a BladeCenter I/O module using the management module Web interface.

**Note:** The I/O-module configuration pages vary by I/O-module type. Each page displays only those settings that apply to the I/O module that is installed; therefore, some steps in the following procedure might not apply to your I/O module.

Most I/O-module configuration is performed through the management interface that is provided by each I/O module. Before you can access this management environment through a Web browser, some I/O modules must have their communications parameters set up through the management-module Web interface or through the management-module command-line interface.

This section has general instructions for configuring I/O-module communications parameters by using the management-module Web interface. See the *Installation Guide* for your I/O module for specific configuration information. Instructions for configuring the I/O module by using the management-module command-line interface are in the *BladeCenter Management Module Command-Line Interface Reference Guide*.

To configure the I/O module for external communication by using the management-module Web Interface, complete the following steps:

1. Log on to the management module as described in “Connecting to the management module” on page 5. The management-module window opens.
2. From the **I/O Module Tasks** menu, click **Configuration**.
3. In the **I/O Module Configuration** section, click the bay number that corresponds to the location of the I/O module that you are configuring. The applicable bay number is displayed at the bottom of the window, followed by other related I/O-module information, including the IP address. The I/O-module information is divided into two sections: Current IP Configuration and New Static IP Configuration.

4. In the **IP address** field in the **New Static IP Configuration** section, type the new IP address of the I/O module; then, click **Save**. You can set up the IP address for the Gigabit Ethernet switch module in either of two ways:
  - Use the default IP address
  - Obtain a valid, unique IP address from your system administrator

**Note:** The IP address of the I/O module must be on the same subnet as the management module. The management module does not check for invalid IP addresses.

5. Click **Advanced Management** and make sure that the following switch-module features are enabled:
  - External ports
  - External management over all ports
  - Preserve new IP configuration on all resets

The default setting is **Disabled** for these features. If these features are not already enabled, change the setting to **Enabled**; then, click **Save**.

**Note:** See the *Installation and User's Guide* for your BladeCenter unit for additional information about enabling external management over all ports.

6. For I/O modules that support Network Address Translation (NAT) table, click **Network Protocol Configuration**. The first column of the NAT table contains links that you can use to configure the protocol values. The maximum number of protocols is 10. Five protocols are predefined; for example, the first protocol is always hypertext transfer protocol (HTTP), and the second protocol is always Telnet.

You can activate or modify the Network Protocol settings on this page of the management-module interface by clicking one of the following buttons:

- To activate all of the values in the NAT table, click **Activate**.
- To immediately reset all of the values in the NAT table to their defaults, click **Reset to defaults**.

You can now start a Web-interface session, a Telnet session, or a Secure Shell (SSH) session to the I/O module to perform additional configuration. See the documentation for your I/O module for information.



---

## Chapter 3. Management-module Web interface overview

The following topics contain information about the structure and content of the management-module Web interface:

- Features of the management-module Web interface that can be accessed by users, according to their assigned roles or authority levels (see “Web interface pages and user roles”)
- Descriptions of the management-module Web interface pages (see “Management-module Web interface options” on page 52)

See Chapter 2, “Using the management-module Web interface,” on page 5 for information about using the management-module Web interface to perform selected functions.

The Web-based user interface communicates with the management and configuration program that is part of the firmware that comes with the management module. You can use this program to perform the following tasks:

- Defining the login IDs and passwords.
- Selecting recipients for alert notification of specific events.
- Monitoring the status of the BladeCenter unit, blade servers, and other BladeCenter components.
- Controlling the BladeCenter unit, blade servers, and other BladeCenter components.
- Accessing the I/O modules to configure them.
- Changing the startup sequence in 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 removable-media drives and USB ports. (The removable-media drives in the BladeCenter unit are viewed as USB devices by the blade server operating system.)
- Setting the active color of the critical (CRT) and major (MJR) alarm LEDs (for BladeCenter T unit only).

You also can use the management-module Web interface, SNMP, and the management-module command-line interface to view some of the blade server configuration settings. For more information, see the information in this chapter and the documentation for the management method that you are using.

---

### Web interface pages and user roles

Different user authority levels are needed to access different pages in the management module Web interface.

Some fields and selections in the management-module Web interface pages can be changed or executed only by users who are assigned roles with the required level of authority for those pages. Users with the Supervisor role (command authority) for a page can change information and execute all tasks in the page. Viewing

information does not require any special command authority; however, users can be assigned restricted read-only access to specific devices in the BladeCenter unit, as follows:

- Users with the Operator role can view all information.
- Users with the Chassis Operator custom role can view information about the common BladeCenter unit components.
- Users with the Blade Operator custom role can view information about the blade servers.
- Users with the I/O Module (Switch) Operator custom role can view information about the I/O modules.

Table 2 lists the management-module Web interface pages and the roles (command authority levels) that are required to change information in these pages. The pages and roles that are listed in this table apply only to changing the information in a page or executing a task specified in a page: viewing the information in a page does not require any special role or command authority. In the table, each row indicates the valid user roles (command authorities) that enable a user to change the information or execute a task in that page. For example, in Table 2 executing tasks in the **Blade Tasks** → **Power/Restart** page is available to users with the Supervisor role or to users with the Blade Administration role.

**Important:** Make sure that the role that is set for each user is correct after you update management-module firmware, because these definitions might change between firmware versions.

Table 2. User role relationships

Page	Role required to change information or execute tasks										
	Supervisor	Chassis User Account Management	Blade Server Remote Presence	Chassis Operator	Chassis Administration	Blade Administration	I/O Module Administration	Chassis Log Administration	Chassis Configuration	Blade Configuration	I/O Module Configuration
<b>Monitors</b>											
System Status	•	•	•	•	•	•	•	•	•	•	•
Event Log (view)	•	•	•	•	•	•	•	•	•	•	•
Event Log (clear or set log policy)	•							•			
LEDs	•	•	•		•	•	•	•	•	•	•
Fuel Gauge	•	•	•		•	•	•	•	•	•	•
Hardware VPD	•	•	•		•	•	•	•	•	•	•
Firmware VPD	•	•	•		•	•	•	•	•	•	•
<b>Blade tasks</b>											
Power/Restart	•					•					
Remote Control (remote console)	•		•								

Table 2. User role relationships (continued)

Page	Role required to change information or execute tasks										
	Supervisor	Chassis User Account Management	Blade Server Remote Presence	Chassis Operator	Chassis Administration	Blade Administration	I/O Module Administration	Chassis Log Administration	Chassis Configuration	Blade Configuration	I/O Module Configuration
Remote Control (virtual media)	•		•								
Firmware Update	•					•					
Configuration	•									•	
Serial Over LAN	•								•	•	
<b>I/O-module tasks</b>											
Admin/Power/Restart	•						•				
Configuration (see Note 1)	•										•
Firmware Update	•						•				
<b>MM control</b>											
General Settings	•								•		
Login Profiles	•	•									
Global Login Settings	•								•		
Alerts (see Note 2)	•								•		
Port Assignments	•								•		
Network Interfaces	•								•		
Network Protocols	•								•		
Security	•								•		
Configuration File (backup)	•			•							
Configuration File (restore)	•										
Firmware Update	•				•						
Restore Defaults (see Note 3)	•				•				•		
Restart MM	•				•						

**Notes:**

1. To send ping requests to an I/O module (**Advanced Management** link in **I/O Module Tasks → Configuration** page), the I/O Module Administration, I/O Module Configuration, or I/O Module Operator role is required.
2. For the BladeCenter T Management Module, the Supervisor or Chassis Administration role is required to reset filter detection under **MM Control → Alerts**.

3. For the **MM Control → Restore Defaults** page, both the Chassis Administration and Chassis Configuration roles are required.

---

## Management-module Web interface options

Run the management and configuration program from the management-module Web interface to 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). The links that are in the navigation pane are described in the following sections.

Online help is provided for the management-module Web interface. Click the help icon next to a section heading to display additional information about that item.

## Monitors

Select the choices in **Monitors** to view the status, settings, and other information about components in your BladeCenter unit.

### System Status

Select **Monitors → System Status** 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 in the BladeCenter unit.

The following page is displayed.

---

#### System Status Summary

 System is operating normally. All monitored parameters are OK.

The following links can be used to view the status of different components.

[Blades](#)  
[I/O Modules](#)  
[Management Modules](#)  
[Power Modules](#)  
[Fan-packs](#)  
[Blowers](#)  
[Front Panel](#)

---

## BladeCenter T alarm management:

Select this page to manage alarms for BladeCenter T units.

---

**System Status Summary** 

 One or more monitored parameters are abnormal.

**Critical Alarms**

Alarm Description	Action
Power Supply 4 DC Good Fault	<input type="button" value="ACK"/> <input type="button" value="CLEAR"/>

**Major Alarms**

Alarm Description	Action
Insufficient chassis power to support redundancy	<input type="button" value="ACK"/> <input type="button" value="CLEAR"/>

**Minor Alarms**

Alarm Description	Action
power will be cycled at 2AM - sysadmin	<input type="button" value="ACK"/> <input type="button" value="CLEAR"/>

**Acknowledged Alarms**

Alarm Description	Action
filter will need changing during next service	<input type="button" value="CLEAR"/>

The following links can be used to view the status of different components.

[Blade Servers](#)  
[I/O Modules](#)

For the BladeCenter T unit, the System Status Summary displays active alarm conditions that are grouped by alarm type (critical, major, or minor). A critical, major, or minor alarm lights the LED that is associated with its alarm level on the BladeCenter T unit. Acknowledging an alarm moves it from the critical, major, or minor active list to the acknowledged list and turns off its LED. Clearing an alarm removes it from all alarm lists and turns off its LED. Acknowledging or clearing an alarm turns off its LED only when no other alarms of the same level are active to keep the LED lit.

There are two action push buttons, **ACK** and **CLEAR**, next to each alarm description in the list of active alarms. Click **ACK** to turn off the LED that is associated with an alarm and move the alarm to the acknowledged list. Click **CLEAR** to turn off the LED that is associated with the alarm and remove the alarm from all alarm lists. After an alarm has been moved to the acknowledged list, you can remove it from all alarm lists by clicking the **CLEAR** action push button that is to the right of the acknowledged alarm description.

## BladeCenter unit detailed component status:

Select **Monitors** → **System Status** to view detailed component status information.

The System Status page provides the following detailed status information for BladeCenter components.

The following illustration shows a blade server status page

**Blades** ⓘ

Click the icon in the Status column to view detailed information about each blade server.

Bay	Status	Name	Pwr	Owner**		Network		WOL	Local Control			BEM†
				KVM	MT	Onboard	Card		Pwr	KVM	MT	
1	●	SNMk10V7383140	Off			Eth	---	On	X	X	X	
2	●	SNMk10V7364105	Off			Eth	---	On	X	X	X	
3	●	Blade 04	Off			Eth	---	On	X	X	X	
4		No blade present										
5		No blade present										
6	●	SNMk10L1063166	Off	X	X	Eth	---	On	X	X	X	
7		No blade present										
8		No blade present										

\* MT = Media Tray (CD/USB), WOL = Wake on LAN, BEM = Blade Expansion Module.  
 † BSE = Blade Storage Expansion, BPE = Blade PCI Expansion  
 \*\* You can change the KVM and Media Tray ownership on the Remote Control panel (under Blade Tasks)

When you click **Blade servers**, the following information is displayed:

- **Bay:** The lowest-number bay that the blade server occupies.
- **Status:** An icon that indicates good , warning , or critical  status of the power-module cooling device. Click the icon for more detailed status information.
- **Name:** The name of the blade server once it has successfully completed initialization. Before the blade server achieves that state, it might display one of the following text strings:
  - **Discovery:** The blade server is still undergoing initialization
  - **Comm Error:** The blade server is having a problem communicating with the management module
  - **Kernel Mode:** The blade server has failed its initialization and is in a reduced function state
- **Pwr:** The power state (on or off) of the blade server.
- **Owner:** An indication of whether the current blade server owns the following BladeCenter resources:
  - **KVM:** Keyboard, video, and mouse
  - **MT:** The media tray that contains the removable-media drives and USB ports
- **Network:** An indication of which network interfaces are on the blade server (Onboard) and the I/O expansion options (Card). 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.
- **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 the blade server BIOS 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 that are made in the management module override the settings in the blade server BIOS. See “Power/Restart” on page 66 for information.

**Note:** If a blade server does not support the Wake on LAN feature, this field displays a value of n/a.

- **Local Control:** An indication of whether the following options are enabled:
  - Local power control
  - Local keyboard, video, and mouse switching
  - Local removable-media drive and USB port switching
- **BEM:** An indication of whether an expansion unit, such as a SCSI expansion unit or PCI I/O Expansion Unit, occupies the blade bay.

The following illustration shows an I/O Modules status page.

**I/O Modules** 

Bay	Status	Type*	MAC Address	IP Address	Pwr	POST Status
1		Ethernet SM	00:05:5D:89:A3:A0	192.168.70.127	On	POST results available: FF: Module completed POST
2			No module present			
3			No module present			
4			No module present			

\* SM = Switch Module, CM = Concentrator Module, PM = Pass-thru Module

When you click **I/O Modules**, the following information is displayed. The number of I/O module bays varies by BladeCenter unit type.

- **Bay:** The number of the bay that the I/O module occupies.
- **Status:** An icon that indicates good, warning, or bad status for the I/O module. Click this icon to view I/O compatibility status information.
- **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, do not have a MAC address or an IP address.

- **IP Address:** The IP address of the I/O module.
- **Pwr:** The power state (on or off) of the I/O module.
- **POST Status:** Text information about the status of the I/O module.

**Management Modules** 

Click the icon in the Status column for details about the primary management module.

Bay	Status	IP Address (external n/w interface)	Primary
1		192.168.70.125	X
2		No MM present	

When you click **Management Modules**, the following information is displayed:

- **Bay:** The number of the bay that the management module occupies.
- **Status:** An icon that indicates good , warning , or critical  status of the power-module cooling device. Click the status icon for more detailed status information, such as self-test results, power-supply voltage levels, the inside temperature of the BladeCenter unit, and a list of users who are currently logged in to the BladeCenter unit.
- **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	Status	Details
1		Power module status OK
2		Power module status OK
3		No power module
4		No power module

When you click **Power Modules**, the following information is displayed:

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

**Blowers** 

Bay	Status	Speed (% of max)
1		89%
2		94%

When you click **Blowers**, the following information is displayed:

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

## Media Tray ?

Bay	Temp (°C)	Warning	Warning Reset
1	22.00	39.00	30.00

When you click **Media Tray** the following information is displayed (media tray temperature status is not available for all BladeCenter unit types):

- **Temp (C°)**: The ambient temperature of the media tray, as indicated by the front-panel temperature sensor.
- **Warning**: The ambient temperature threshold of the media tray at which a temperature warning event is entered in the event log.
- **Warning Reset**: The ambient temperature threshold of the media tray. If the temperature exceeds the warning threshold and afterwards drops below the warning reset threshold, the temperature warning event is cleared. An indication that the temperature warning is cleared is entered in the event log.

## Event Log

Select **Monitors** → **Event Log** to view entries that are currently stored in the management-module event log.

The screenshot shows the 'Event Log' window with a 'Monitor log state events' checkbox checked. It features a filter section with 'Severity' (Error, Warning, Info), 'Source' (BLADE\_02, BLADE\_05, SERVPROC), and 'Date' (06/23/03) dropdowns, along with 'Filter' and 'Disable Filter' buttons. A note indicates that Ctrl is used for multiple selections and Shift for ranges. Below the filters, it says 'Filters: None'. The main table contains six entries, with the first three being errors (E) and the last three being information (I). The log ends with 'End of Log.' and has 'Clear Log' and 'Save Log as Text File' buttons at the bottom.

Index	Sev	Source	Date/Time	Text
1	E	BLADE_02	06/23/03, 06:16:06	(IBM 867821X SN1) Hard Drive 2 Fault
2	E	BLADE_05	06/23/03, 06:15:08	(SN#J1RNE34911N) POSTBIOS: 162 Configuration Change Has Occurred
3	E	BLADE_05	06/23/03, 06:15:08	(SN#J1RNE34911N) POSTBIOS: 1762 Configuration Change Has Occurred
4	I	SERVPROC	06/23/03, 06:14:10	User USERID attempting to restart blade in bay 2.
5	I	SERVPROC	06/23/03, 06:13:55	User USERID attempting to restart blade in bay 5.
6	I	SERVPROC	06/23/03, 06:13:41	System log cleared.

This log includes entries for events that are detected by the BladeCenter unit and installed components. 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 it is configured to do so.

The following sources can generate events that are recorded in the event log:

- Baseboard Management Controller (BMC) (POSTBIOS)

- BladeCenter unit (SERVPROC)
- Blade device by bay number (Blade\_XX)

**Notes:**

- XX in an event source refers to the bay number of the reporting device.
- BladeCenter T units generate alarms with severities of critical, major, and minor. For the purposes of the management module event log, critical and major alarms are written to the log as errors, and minor alarms are written as warnings. Alerts are assigned severity ratings of Error, Warning, and Information.

The event log is of fixed capacity. On the BladeCenter unit, when the log is 75% full, the BladeCenter Information LEDs are lit. On the BladeCenter T unit, when the log is 75% full, the BladeCenter T MNR (minor alarm) LED is lit. On the BladeCenter unit, when the log is full, new entries overwrite the oldest entries, and the BladeCenter Error LEDs are lit. On the BladeCenter T unit, when the log is full, new entries overwrite the oldest entries, and the BladeCenter T MJR (major alarm) LED is lit. If you do not want the management module to monitor the state of the event log, clear the **Monitor log state events** check box 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 **Monitors** → **LEDs** to manage LED behaviors for Telco and other BladeCenter units.

### BladeCenter unit LEDs:

Select **Monitors** → **LEDs** to manage the LED behavior for the BladeCenter unit.

---

## BladeCenter LEDs

Use the following links to jump down to different sections on this page.

[Media Tray and Rear Panel LEDs](#)

[Blade LEDs](#)

[I/O Module LEDs](#)

[Power Module Cooling Device LEDs](#)

[Chassis Cooling Device LEDs](#)

---

Select **LEDs** 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 flash the location LED on the BladeCenter unit and the blade servers.

The following information is displayed.

### Media Tray and Rear Panel LEDs [?](#)

LED	Status	Action
System error		
Information		<input type="button" value="Off"/>
Temperature		
Location		<input type="button" value="On"/> <input type="button" value="Off"/> <input type="button" value="Blink"/>

- **Media Tray LEDs:** The state of the following LEDs on the BladeCenter system LED page. You can change the state of the information and location LEDs.
  - System error
  - Information
  - Over temperature
  - Location

### Blade LEDs [?](#)

Click the hyperlinks in the Name column to view detailed LED state information about a specific blade.

Bay	Name	Pwr*	Error	Information	KVM	MT	Location
1	<a href="#">SN#YL31W713500</a>	Off		<input type="button" value="Off"/>			<input type="button" value="On"/> <input type="button" value="Off"/> <input type="button" value="Blink"/>
2	<a href="#">SN#YL31W7135008</a>	Off		<input type="button" value="Off"/>			<input type="button" value="On"/> <input type="button" value="Off"/> <input type="button" value="Blink"/>
3	No blade present						
4	No blade present						
5							
6	<a href="#">SN#YK30A0642036</a>	Off		<input type="button" value="Off"/>			<input type="button" value="On"/> <input type="button" value="Off"/> <input type="button" value="Blink"/>
7	No blade present						
8	No blade present						
9	No blade present						
10	No blade present						
11	No blade present						
12	No blade present						
13	No blade present						
14	No blade present						

\* If a blade is powered off, its physical LEDs are not lit. This table represents the status of all LEDs, even for powered-off blades.

- **Blade LEDs:** The state of the following LEDs on the blade server control page. You can change the state of the information and location LEDs.
  - Power
  - Error
  - Information
  - Keyboard, video, and monitor select
  - Media (optical drive, diskette drive, USB port) select
  - Location
- **I/O-Module LEDs:** The state of the LEDs on some I/O modules.

## BladeCenter T alarm management:

Select **Monitors** → **LEDs** to view and manage alarms for the BladeCenter T units.

The screenshot displays the 'LEDs' management interface. It is divided into three main sections:

- Front and Rear Panel LEDs:** A table with columns for LED, Status, and Action. The 'LED' column lists Critical Alarm, Major Alarm, Minor Alarm, and Location. The 'Status' column shows indicator lights. The 'Action' column includes radio buttons for 'Color of Critical and Major LEDs' (Red or Amber) and buttons for 'On', 'Off', and 'Blink'. Below the table are radio buttons for 'Light LEDs for Most Severe Alarm Only or for All Alarm Levels' (Most Severe Alarm Only or All Alarms).
- Set Alarm Panel LEDs:** A form with a dropdown for 'Alarm Panel Severity' (set to 'Minor') and a text input for 'Alarm Description'. A 'Set' button is located to the right.
- Blade LEDs:** A section with a navigation bar containing 'Home', 'Monitors', 'LEDs', 'Information', 'VMM', 'MT', and 'Location'.

Select **LEDs** to view the state of the BladeCenter T system-status page and blade server control panel LEDs. You also can use this choice to turn on, turn off, or flash the location LED on the BladeCenter unit and the blade servers, and control how the LEDs respond to alarms.

The following information is displayed:

- **Media Tray and Rear Panel LEDs:** Controls and displays the state of the following LEDs on the BladeCenter T system LED panel:
  - Critical Alarm (CRT LED)
  - Major Alarm (MJR LED)
  - Minor Alarm (MNR LED)
  - Location

You can change the state of the location LED and select the active LED color (red or amber) for the critical and major alarm LEDs. This color selection is applied to the LEDs on the front and rear of the BladeCenter T unit and to the LED indications that are shown on this page. You can also specify whether the management module lights LEDs for all alarm levels that occur (critical, major, or minor) or whether it lights only the LED that corresponds to the most severe alarm level that occurs. Amber is the default color of the critical and major alarm LEDs. The management module is also set to light the LEDs for all alarm levels that occur (critical, major, or minor), by default.

- **Set Alarm Panel LEDs:** You can control the status of the LEDs on the front and rear of the BladeCenter T unit by using the alarms database of the management module. Alarms can be added to the alarms database to provide user-defined control. To add an alarm, you must select the alarm severity that specifies which LED the alarm controls and enter a non-blank alarm description; then, click **Set**. After an alarm is added to the database, you can manage the alarm and its associated LED from the System Status page by using the **ACK** and **CLEAR** push buttons (see “System Status” on page 52 for information).

- **Blade 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 (optical drive and USB port) select
  - Location
- **I/O-Module LEDs:** The state of the LEDs on some I/O modules.
- **Hardware Component LEDs:** The state of the LEDs on some BladeCenter hardware components. Some components include a FRU ready for removal LED; the status of this LED is shown in the Safe to Remove column.

## Fuel Gauge

Select **Monitors** → **Fuel Gauge** to view the power information, based on projected power consumption, for each power domain of the BladeCenter unit.

Click the **Power management policy settings** link to go to the section of the **Blade Tasks** → **Configuration** page where you configure power management for the BladeCenter unit (see “Configuration” on page 69 for information).

---

### BladeCenter Power Summary

	Power Domain 1	Power Domain 2
<b>Status</b>	● Power domain status is good.	● Power domain status is good.
<b>Power Modules</b>	Bay 1: 2000W Bay 2: 2000W	Bay 3: 1800W Bay 4: 1800W
<b>Power Management Policy</b>	Non-redundant	Non-redundant
<b>Total Power †</b>	2000W	1800W
<b>Power in Use</b>	390W	0W

### BladeCenter Power Planning

	Power Domain 1	Power Domain 2
<b>Total Power †</b>	2000W	1800W
<b>- Allocated Power (Max)</b>	390W	0W
<b>= Remaining Power</b>	1610W	1800W

† **Note:** Actual total power limit may vary from power module label.

Use the following links to jump to different sections.

[Power Domain 1 details](#)

[Power Domain 2 details](#)

[Power management policy settings](#)

Refresh

---

There are two power domains in the BladeCenter unit. Click **Power Domain 1 details** or **Power Domain 2 details** for the list of BladeCenter components in each power domain (see detailed power status for information). The power-management policy settings determine how the BladeCenter unit reacts in each power domain

to a power-source failure or power-module failure. The combination of the BladeCenter configuration, power-management policy settings, and available power might cause blade servers to reduce their power levels (throttle) or not turn on.

The following power status information is displayed in the **BladeCenter Power Summary** and **BladeCenter Power Planning** sections:

- **Status:** This field contains a color-coded icon that indicates status of the power domains and a short status description that lists any outstanding issues that are related to power consumption or redundancy in each power domain.
- **Power Modules:** This field lists the power modules that are installed in each power domain and their rated capacity, in watts.
- **Power-Management Policy:** This field displays the power-management policy that is set for each power domain, defining how the power domain will react to conditions that might result in a loss of redundancy. This setting is configured on the **Blade Tasks** → **Configuration** page (see “Configuration” on page 69 for information).
- **Power in Use:** This field displays the current power that is being used in each power domain, in watts.
- **Total Power:** This field displays the amount of power that is available in each power domain, in watts. Total power is calculated by the management module according to the rated capacities of the power modules that are installed in a power domain and the power-management policy that has been set for the power domain.
- **Allocated Power (Max):** This field displays the total amount of power, in watts, that is reserved for use by the components that are installed in a power domain. This value might include power for components that are not currently installed in the BladeCenter unit, such as the I/O modules. Power is reserved for these components because the management module preallocates power for some components that are normally required for BladeCenter unit operation. The reserved-power total might also include power for components that are installed in the BladeCenter unit, are in a standby state, and are not turned on. These components are included in the total so that the amount of spare (unallocated) power in the power domain can be accurately calculated.
- **Remaining Power:** This field displays the amount of unallocated (spare) power in a power domain, in watts. This value is used by the management module when it determines whether a newly installed module should turn on. The remaining power value is calculated according to the total power and the amount of reserved power for each power domain.

## Detailed power information:

The detailed power status information for each monitored BladeCenter component is displayed in the **Power Domain details** section of the **Monitors → Fuel Gauge** page.

### Power Domain 1

Bay(s)	Status	Module	State	Allocated Power			CPU Duty Cycles
				Currently	Max	Min	
<i>Chassis Components</i>							
		Midplane	On	10W	10W	10W	n/a
		Media Tray	On	10W	10W	10W	n/a
<i>Blowers</i>							
1		Blower 1	On	120W	120W	120W	n/a
2		Blower 2	On	120W	120W	120W	n/a
<i>Management Modules</i>							
1		WMN189277931	On	25W	25W	25W	n/a
2		Backup MM <i>(not present)</i>		15W	15W	15W	n/a
<i>I/O Modules</i>							
1		Ethernet SM	On	45W	45W	45W	n/a
2		Ethernet SM	On	45W	45W	45W	n/a
<i>Blade Servers</i>							
1		SN#J1RNE77931M	Standby	30W	202W	138W	( 0% ,0% )
2		SN#J1RNE34912M	On	150W	150W	150W	n/a
4		SN#J1RNE18927M	Standby	40W	150W	150W	n/a
<b>DOMAIN TOTALS</b>				<b>Currently</b>	<b>Max</b>	<b>Min</b>	
<b>Power Allocation</b>				610W	892W	828W	

† This blade may throttle if redundancy is lost in this power domain.

\* Cannot communicate with the blade. The power values for this blade are assumed.

Refresh

The BladeCenter components that are part of each power domain are grouped by type. The status information for power domain 1 is shown. There is a separate status section for each power domain in your BladeCenter unit.

The following information is displayed for each component that is installed in a power domain:

- **Bay:** This field displays the bays, if applicable, that a BladeCenter component occupies. It also indicates whether a blade server can reduce its power consumption (throttle) if power redundancy is lost.
- **Status:** This field displays an icon that indicates power-management events that are outstanding for the component. The  icon indicates that a blade server will not be able to turn on because there is not enough remaining power in the power domain to support it. The  icon indicates that a blade server is currently reducing its power consumption (power throttling) to maintain redundant power in a power domain.
- **Module:** This field displays the component description.
- **State:** This field displays the power state of the module (On or Standby).
- **Currently Allocated Power:** This field displays the amount of power, in watts, that is allocated to the module.
- **Maximum Allocated Power:** This field displays the maximum amount of power, in watts, that a component requires.

- **Minimum Allocated Power:** This field displays the minimum amount of power, in watts, that a blade server requires when it is operating at its minimum power level (fully throttled).
- **CPU Duty Cycles:** This field applies only to blade servers. It displays the duty cycle of each microprocessor in a blade server, as a percentage of full operation. The duty cycles of the microprocessors are separated by commas. For each blade server that does not report its duty cycles, n/a is displayed. A duty cycle is a ratio of actual processing time expressed as a percentage of total available processor time.
- **DOMAIN TOTALS:** These fields list the total power that is allocated for all components in the power domain.

## Hardware VPD

Select **Monitors** → **Hardware VPD** to view the hardware vital product data for the BladeCenter unit.

The following illustration shows the Hardware VPD page.

**BladeCenter System VPD**

<b>Type / Model</b>	87301XZ
<b>Serial no.</b>	23A0001
<b>UUID</b>	A7FB FB81 DB12 11D6 8D71 C8D6 4BF2 EDOC

[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	FRU Serial No.
<b>Chassis and Media Tray</b>									
	Chassis	IBM	87301XZ	----	2	4603	90P3678	90P3696	3471CHT
1	Media Tray	----	n/a	n/a	0	----	----	----	----
<b>Blade Servers</b>									
3-4	Blade 04	Intel	883931X	23A0119	----	----	----	90P0978	----
	Daughter Card	Unable to read VPD.							
	Daughter Card	Unable to read VPD.							
5	SN#K10V7363140	SLRM	867841X	KPHT239	8	2303	73P9120	73P9121	K10V736
6	SN#K10UJ353166	SLRM	867841X	KPHT163	8	1803	71P8790	59P6610	K10UJ35
8	SN#K10V7364105	SLRM	867841X	KPHT213	8	2303	73P9120	73P9121	K10V736

Select **Monitors** → **Hardware VPD** 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. The hardware VPD that is collected and stored varies by BladeCenter unit type.

Click a **Module Name** to display a page of additional inventory and port information. This can include the machine type or model number, serial number, and Universally Unique Identifier (UUID) MAC address.

## Firmware VPD

Select **Monitors** → **Firmware VPD** to view the firmware vital product data for the BladeCenter unit.

The following illustration shows the Firmware Vital Product Data (VPD) page.

### Blade Server Firmware VPD

Bay(s)	Name	Firmware Type	Build ID	Released	Revision
1	SN#J1RNE34911N	BIOS	BSE105AUS	06/23/2003	1.00
		Diagnostics	BSYT06AUS	05/01/2003	1.00
		Blade sys. mgmt. proc.	BR8T17A	n/a	17
2	SN#ZJ1WLW47T16N	BIOS	BWE105AUS	08/06/2004	1.00
		Diagnostics	BWYT01AUS	06/11/2004	1.00
		Blade sys. mgmt. proc.	BWBT02A	n/a	0

To reread firmware VPD for a blade, select the blade, and click "Reload VPD". This process may take a while.

Target

### I/O Module Firmware VPD

Bay	Type	Firmware Type	Build ID	Released	Revision
1	Ethernet SM	Boot ROM	BRESMB4G	02/21/2003	05
		Main Application 1	BRESMR4G	12/19/2003	81
2	Ethernet SM	Boot ROM	BRESMB4G	01/29/2003	04
		Main Application 1	BRESMR4G	10/16/2003	72

### Management Module Firmware VPD

Bay	Name	Firmware Type	Build ID	File Name	Released	Revision
1	4P3MM	Main application	BRET72A	CNETMNUS.PKT	08-13-04	16
		Boot ROM	BRBR72A	CNETBRUS.PKT	08-13-04	16
		Remote control	BRRG72A	CNETRGUS.PKT	08-13-04	16
2	Redundant MM	Main application	BRFT72A	CNETMNUS.PKT	08-13-04	16

Click **Firmware Vital Product Data** 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 that is collected and stored varies by BladeCenter unit type.

The firmware VPD includes the firmware type and version information such as a build ID, release date, and revision number. The VPD information varies by BladeCenter component type; for example, the VPD for the management-module firmware might also include the file name of the firmware components. (After you select **Firmware Vital Product Data**, it takes up to 30 seconds to refresh and display information.)

Click **Reload VPD** to refresh the firmware VPD information for a selected blade server or for all blade servers in the BladeCenter unit.

## Blade Tasks

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

### Power/Restart

Select **Blade Tasks** → **Power/Restart** to turn individual blade servers on and off, or to restart them.

#### Blade Power / Restart <sup>2</sup>

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

<input type="checkbox"/>	Bay	Name	Pwr	Local Pwr Control	Wake on LAN	Console Redirect
<input type="checkbox"/>	1	SN#ZJ1YYT52N040	On	Enabled	On	
<input type="checkbox"/>	2	SN#K10UJ32F23U	On	Enabled	On	
<input type="checkbox"/>	3	SN#ZK118252E1AP	On	Enabled	On	
<input type="checkbox"/>	4	SN#K10WE39F158	Off	Enabled	On	
<input type="checkbox"/>	5	SN#ZK11VM5CB104	Off	Enabled	On	
	6	No blade present				
	7	No blade present				
	8	No blade present				
	9	No blade present				
	10	No blade present				
	11	No blade present				
	12	No blade present				
	13	No blade present				
	14	No blade present				

[Power On Blade](#)

[Power Off Blade](#)

[Shut Down OS and Power Off Blade](#)

[Restart Blade](#)

[Restart Blade with NMI](#)

[Enable Local Power Control](#)

[Disable Local Power Control](#)

[Enable Wake on LAN](#)

[Disable Wake on LAN](#)

[Restart Blade System Mgmt Processor](#)

The following operations can be executed only on some POWER-based blades.

[Restart Blade and clear NVRAM](#)

[Restart Blade with Diagnostic Boot](#)

[Restart Blade with Diagnostic Boot and Default Bootlist](#)

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

- Turn on or turn off the selected blade server (set the power state on or off).
- Shut down the operating system and power off the blade server.
- Restart the blade server, with or without a non-maskable interrupt (NMI).
- 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 (indicated by an X in the Console Redirect column).

The following operations can be performed on some POWER-based blade servers.

- Restart the selected blade server and clear NVRAM.
- Restart the selected blade server and run diagnostics.

- Restart the selected blade server and run diagnostics, using the default boot sequence that is configured for the blade server.

## Remote Control

Select **Blade Tasks** → **Remote Control** to operate a blade server from a networked remote console.

The following illustration shows the remote-control page.

---

**Remote Control Status** ⓘ

KVM owner:	Blade5 - SN#J1RNE34911N since 11/15/2003 09:24:11
Media tray owner:	Blade2 - IBM 867821X SN1 since 11/10/2003 10:12:57
Console redirect:	No session in progress.

---

**Start Remote Control** ⓘ

To disable the buttons located on the blade servers for KVM and media tray switching, check the boxes below and click "Save". Click "Start Remote Control" to control a blade server remotely. A new window will appear that provides access to the Remote Console and Remote Disk functionality. On this window, you will have full keyboard and mouse control of the blade server which currently owns the KVM. You will also be able to change KVM and media tray ownership.

**Note:** An Internet connection is required to download the Java Runtime Environment (JRE) if the Java 1.4 Plug-in is not already installed.

Disable local KVM switching  
 Disable local media tray switching

---

Click **Start Remote Control** to establish a remote console. On a remote console, you can 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 special meanings to the blade server. For example, to transmit Ctrl+Alt+Del to the blade server, click the **Ctrl** and **Alt** icons, then press the Del key on the keyboard.

Use the remote console to perform the following tasks:

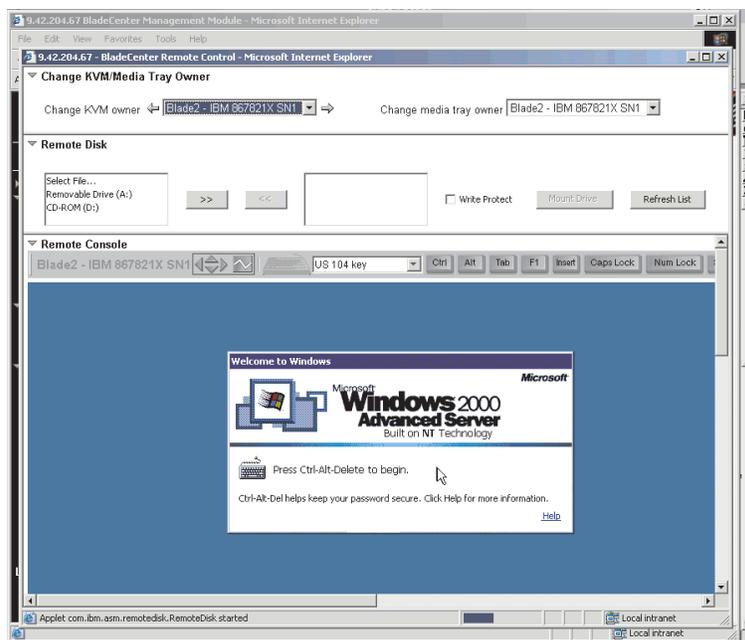
- View and change the blade server that currently controls the keyboard, monitor, and mouse (KVM) and the removable-media drives and USB ports (media tray) in the selected blade server unit. See the *Installation and User's Guide* for your blade server for more information about KVM and media tray switching.

### Notes:

- The operating system in the blade server must provide USB support for the blade server to recognize and use the keyboard and mouse, even if the keyboard and mouse have PS/2-style connectors.
- If the operating system in the blade server does not support remote disk access, this feature is not available.
- If you install a supported Microsoft Windows operating system on the blade server while it is not the current owner of the KVM, a delay of up to 1 minute occurs the first time that you switch the KVM to the blade server. All subsequent switching takes place in the normal KVM switching time frame (up to 20 seconds).

- Select and access the drives in the media tray.
  - Mount a drive or image, from the system that is acting as the remote console, onto a blade server. The mounted drive or image appears as a USB device that is attached to the blade server. See “Using the remote disk feature” on page 44 for information and instructions.
  - Access files at any available network location.
  - View the details of any currently active remote-control session (user ID, client IP address, start time).
  - Enable or disable local switching of the KVM for blade servers until it is explicitly enabled again. This prevents a local user from switching the console to a different blade server while you are performing remote-control tasks. Users with access to the BladeCenter unit can use the KVM select button on a blade server to switch KVM and media tray ownership. Unless you disable local access, they also can use a keyboard that is attached directly to the management module to switch KVM control between blade servers.
- If a local user discovers that there is no response when the KVM select button is pressed, local control might have been disabled on the blade server by a remote user who is using the management module.
- Enable or disable local switching of the media tray for all blade servers until they are explicitly enabled again. This prevents other users from switching control of the media tray to a different blade server while you are performing a task. The media tray is used by one blade server at a time.

The following illustration shows a remote-control session for a management module.



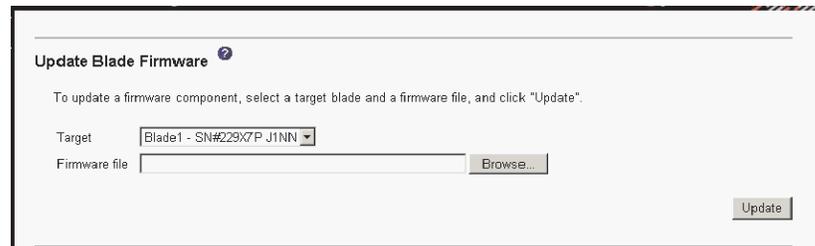
**Note:** To run the Java Remote Console applet from a management module, click **Start → Java Control Panel**; then, click the **Cache** tab and make sure that **Enable Caching** is not selected. Use a Java Virtual Machine (JVM) Plug-in version 1.4.2\_08 or later, but earlier than 1.6.0 (JRE 6.0) installed.

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.

## Firmware Update

Select **Blade Tasks** → **Firmware Update** to update the Blade System Management Processor (BSMP) firmware on a blade server.

Use this page to update the BSMP firmware on a specific blade server. Currently, the blade server BSMP is the only component whose firmware can be updated by using this page. This page does not support the update of blade server BIOS, diagnostics, or network adapter firmware.



Select the target blade server and the firmware file to use for the update; then, click **Update**. You can obtain the firmware files from <http://www.ibm.com/systems/support/>.

## Configuration

Select **Blade Tasks** → **Configuration** to view and change blade server configuration settings.

The following illustration shows blade server configuration choices for a management module.



Bay	Name
1	
2	SNM-K10-73621EB
3	
4	Blade 04
5	SNM-K10-7363140
6	SNM-K10-L053166
7	No blade present
8	SNM-K10-7364105

Click **Blade Information** to perform the following tasks:

- View the bay locations and names of the installed blade servers

## Blade Information ?

Bay	Name
1	SN#YL31W713500
2	SN#YL31W7135008
3	No blade present
4	No blade present
5	SN#YK30A0642036
6	
7	No blade present
8	No blade present
9	No blade present
10	No blade present
11	No blade present
12	No blade present
13	No blade present
14	No blade present

[Advanced Configuration](#)

Save

Click **Blade Policy Settings** to enable or disable the following items on all blade servers in the BladeCenter unit:

### Blade Policy Settings ?

These settings apply to all blade bays (including the empty bays).

Local power control	Enabled <input type="button" value="v"/>
Local KVM control	Enabled <input type="button" value="v"/>
Local media tray control	Enabled <input type="button" value="v"/>
Remote media tray control	Enabled <input type="button" value="v"/>
Multiple concurrent remote video sessions per blade	Disabled <input type="button" value="v"/>
Wake on LAN	Enabled <input type="button" value="v"/>

Save

- **Local power, KVM, and media tray control:** These fields display the global policy setting for all blade bays. When set to **Enabled**, the feature is enabled for all bays. When set to **Disabled**, the feature is disabled for all bays. The value of **Not set** indicates that no global policy has been set; some bays might have the feature enabled while others have it disabled.
- **Remote media tray control:** This field displays the global policy setting for remote media tray switching for all blade bays. When set to **Enabled**, the media tray switching for all bays are enabled on the Remote Control applet. When set to **Disabled**, the media tray switching for all bays are disabled on the Remote

Control applet. The value of **Not set** indicates that no global policy has been set (some bays might have the media tray switching enabled while others have it disabled). If the remote disk feature is disabled, this field will be disabled. You can enable the remote disk by going to the **MM Control → Network Protocols → Remote Control** page.

- **Power management settings.** These fields display the power management settings for management modules.
- **Wake on LAN:** This field displays the global policy setting for Wake on LAN for all blade bays. When set to **Enabled**, Wake on LAN is enabled for all bays. When set to **Disabled**, Wake on LAN is disabled for all bays. The value of **Not set** indicates that no global policy has been set; some bays might have Wake on LAN enabled while others have it disabled. Not all blade server types support the WOL capability; the default BIOS setting for Wake on LAN is **Enabled** for blade servers which support WOL.

Click **Management Network Configuration** to complete the following tasks:

- View a list of blade servers in the BladeCenter unit. This section displays a table which shows all the blade servers in the chassis.

---

**Management Network Configuration** 

VLAN ID

BSMP IP address range

The links in this table will allow users to configure management network interface(s) on some blades. Note that only certain blade types support this configuration.

Bay	Name
1	<a href="#">W03_SLES9</a>
2	<a href="#">SN#YL10W7249025</a>
3	SN#Y1S03377T10B
4	No blade present
5	No blade present
6	W200364
7	RHEL4U464
8	SN#Y1S0MA74R10B
9	W200364b
10	SN#YK3150795022
11	SN#YK339074T15D
12	<a href="#">P6</a>
13	B132-ASPEN
14	<a href="#">P6</a>

---

In order to change the network configuration for a blade server, click on the blade server name link. This will take you to another page where the following settings can be changed and saved. Note that only certain blade servers types support this configuration.

- DHCP
- IP Address
- Subnet mask
- Gateway address

Click **Boot Sequence** to view or define the startup (boot) sequence for one or more blade servers. The startup sequence prioritizes the boot-record sources for a blade server.

## Boot Sequence <sup>?</sup>

Follow the links in the Name column to edit the boot sequence settings of individual blades.

Bay	Name	1 <sup>st</sup> Device	2 <sup>nd</sup> Device	3 <sup>rd</sup> Device	4 <sup>th</sup> Device
1	<a href="#">JS21-31W71</a>	CDROM	Hard Drive 0	Network	No device
2	<a href="#">SH#YL31W7135008</a>	N/A			
3	<a href="#">Vista32_3D</a>	USB Floppy	CDROM	Hard Drive 0	Network
4	Init failed	N/A			
5	No blade present				
6	No blade present				
7	No blade present				
8	No blade present				
9	No blade present				
10	No blade present				
11	No blade present				
12	No blade present				
13	No blade present				
14	No blade present				

The following boot sequences for your BladeCenter unit and blade servers are available:

- **Hard disk drives** (0 through 4). The selection of hard disk drives depends on the hard disk drives that are installed in your blade server.
- **CD-ROM** (optical drive).
- **Diskette drive** (some BladeCenter unit types)
- **Network - PXE**. Selecting Network - PXE attempts a PXE/DHCP network startup the next time the blade server is turned on or restarted.
- **iSCSI boot devices**. Select **iSCSI Critical** to force the blade server to search for an iSCSI boot device until it finds one.

## Serial Over LAN

Select **Blade Tasks** → **Serial Over LAN** to monitor the Serial Over LAN (SOL) status and to enable or disable SOL.

### Serial Over LAN (SOL) <sup>?</sup>

Use the following links to jump down to different sections on this page.

[Serial Over LAN Status](#)  
[Serial Over LAN Configuration](#)

### Serial Over LAN Status <sup>?</sup>

Click the checkboxes in the first column to select one or more blade servers; then, click one of the links below the table to enable or disable SOL on the selected blades.

**Note:** You have to enable the global "Serial over LAN" flag below in the Configuration section before enabling SOL on individual blade servers.

<input type="checkbox"/>	Bay	Name	SOL	SOL Session	BSMP IP Address
<input type="checkbox"/>	1	Blade does not support SOL	n/a	n/a	n/a
<input type="checkbox"/>	2	<a href="#">SN#ZJ11WS447L14E</a>	Enabled	Not ready	10.10.10.81
<input type="checkbox"/>	3	<a href="#">SN#WS1Z147L47S</a>	Enabled	Not ready	10.10.10.82
<input type="checkbox"/>	4	<a href="#">SN#ZJ11WS47L74W</a>	Enabled	Not ready	10.10.10.83
<input type="checkbox"/>	5	No blade present			
<input type="checkbox"/>	6	Blade does not support SOL	n/a	n/a	n/a
<input type="checkbox"/>	7	No blade present			
<input type="checkbox"/>	8	No blade present			
<input type="checkbox"/>	9	No blade present			
<input type="checkbox"/>	10	No blade present			
<input type="checkbox"/>	11	No blade present			

Select **Serial Over LAN** for each blade server and globally for the BladeCenter unit. Enabling or disabling SOL globally does not affect the SOL session status of each blade server; SOL must be enabled both globally for the BladeCenter unit and individually of each blade server on which you plan to start an SOL session. SOL is enabled globally and on the blade servers by default.

---

### Serial Over LAN Configuration ?

Serial over LAN   
SOL VLAN ID   
BSMP IP address range

#### Transport Parameters

Accumulate timeout  msec  
Send threshold  bytes  
Retry count   
Retry interval  msec

#### User Defined Keystroke Sequences

Enter CLI key sequence   
Reset blade key sequence

---

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

Start and run SOL sessions by using the management-module command-line interface. See the *BladeCenter Management Module Command-Line Interface Reference Guide* for information and instructions.

## I/O Module Tasks

Select **I/O Module Tasks** to manage network-interface I/O modules in the BladeCenter unit.

I/O module tasks include:

- “Admin/Power/Restart” on page 74
- “Configuration” on page 75
- “Firmware Update” on page 77

**Note:** Some choices are not available for some types of I/O modules.

## Admin/Power/Restart

Select **I/O Module Tasks** → **Admin/Power/Restart** to view and manage the power status of the I/O modules.

The following illustration shows I/O-module power and restart settings.

**I/O Module Power/Restart** ⓘ

Select one or more module(s) using the checkboxes in the first column and then click on one of the links below the table to perform the desired action.

<input type="checkbox"/>	Bay	Type	MAC Address	IP Address	Pwr	POST Status
<input type="checkbox"/>	1	Ethernet SM	00:05:5D:89:A3:AD	10.90.90.94	On	POST results not complete: AD
<input type="checkbox"/>	2		No module			
<input type="checkbox"/>	3		No module			
<input type="checkbox"/>	4		No module			

[Power On Module\(s\)](#)  
[Power Off Module\(s\)](#)  
[Restart Module\(s\) and Run Standard Diagnostics](#)  
[Restart Module\(s\) and Run Extended Diagnostics](#)  
[Restart Module\(s\) and Run Full Diagnostics](#)

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

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

**I/O Module Advanced Setup** ⓘ

Select a module:

Fast POST:

External ports:

For each I/O module, enable or disable the following features:

- Fast POST
- External ports

## Configuration

Select **I/O Module Tasks** → **Configuration** to view or change the IP configuration of the I/O modules.

**Note:** The content of I/O-module configuration pages varies by I/O-module type. Each page displays only those settings that apply to the I/O module that is installed.

---

### I/O Module Configuration

Use the following links to jump down to different sections on this page.

[Bay 1](#)  
[Bay 2](#)  
[Bay 3](#)  
[Bay 4](#)  
[Bay 5](#)  
[Bay 6](#)  
[Bay 7](#)  
[Bay 8](#)  
[Bay 9](#)  
[Bay 10](#)

---

Select **Configuration**. Links to the configuration section for each I/O module are at the top of the page.

---

### Bay 1 (Ethernet SM)

#### Current IP Configuration

Configuration method: Static  
IP address: 192.168.70.127  
Subnet mask: 255.255.255.0  
Gateway address: 0.0.0.0

#### New Static IP Configuration

Status: Enabled

*To change the IP configuration for this I/O module, fill in the following fields and click "Save". This will save and enable the new IP configuration.*

IP address   
Subnet mask   
Gateway address

[Advanced Configuration](#)

Save

---

### Bay 2 (Server Conn M)

#### Current IP Configuration

Configuration method: Port forwarding  
IP address: 9.42.204.68: <port>  
Subnet mask: 255.255.255.192  
Gateway address: 9.42.204.65

[Advanced Configuration](#) [Network Protocol Configuration](#)

---

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 I/O-module IP address that is in NVRAM, the I/O module uses whatever IP address that is in the I/O module NVRAM. If the two IP addresses are not the same, you might not be able to manage the I/O module anymore. The management module cannot apply the I/O-module IP address from its NVRAM under any of the following conditions:

- The management module is restarting.
- The management module has failed.
- The management module has been removed from the BladeCenter unit.

You must use the Telnet interface to log in to the I/O module, change the IP address to match the one that you assigned through the management module; then, save the I/O-module settings in the Telnet session (**Basic Setup** → **Save Changes**).

For I/O-module communication with a remote management station, 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.

Select **Advanced Configuration** to enable external management, ping an I/O module, configure other advanced I/O-module settings, return an I/O module to the default configuration, and start the configuration and management firmware that might be in an I/O module.

**Notes:**

- The initial factory-defined user ID and password of the I/O-module firmware are as follows:
  - User ID: USERID (all capital letters)
  - Password: PASSW0RD (note the zero, not O, in PASSW0RD)
- If your I/O module supports secure Web sessions and a Network Address Translation (NAT) table, these must be configured in the Network Address Translation (NAT) table in the **Network Protocol Configuration** page.

---

**Network Protocol Settings** 

To configure a protocol, click a link in the "Protocol Name" column.

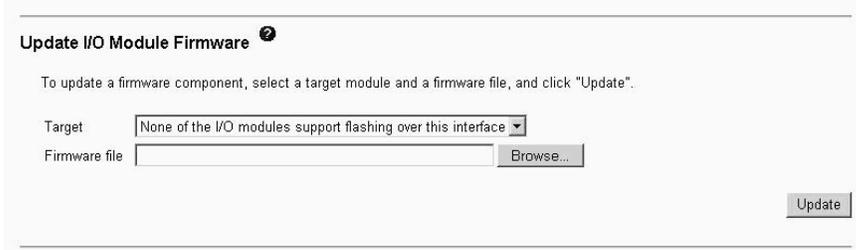
	Protocol Name	Protocol ID	External Port	Internal Port	Enabled
1.	<a href="#">HTTP</a>	TCP	2080	80	Yes
2.	<a href="#">TELNET</a>	TCP	2023	23	Yes
3.	<a href="#">HTTPS</a>	TCP	2443	443	Yes
4.	<a href="#">SSH</a>	TCP	2022	22	Yes
5.	<a href="#">SNMP</a>	UDP	2161	161	Yes
6.	<a href="#">~not used~</a>				
7.	<a href="#">~not used~</a>				
8.	<a href="#">~not used~</a>				
9.	<a href="#">~not used~</a>				
10.	<a href="#">~not used~</a>				

Select **Network Protocol Configuration** to set the network protocol configuration for an I/O module that supports a Network Address Translation (NAT) table. Click **Activate** for the changes to take effect.

See the *Installation and User's Guide* for your BladeCenter unit and "Configuring an I/O module" on page 46 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 *Documentation* CD for your BladeCenter unit.

## Firmware Update

Select **I/O Module Tasks** → **Firmware Update** to update the I/O-module firmware.



**Note:** Firmware update is available only for some I/O-module types.

Select **Firmware Update** 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 <http://www.ibm.com/systems/support/>.

## MM Control

Select the **MM Control** choices to view and change the settings or configuration on the management module that you are logged in to (the primary management module) through the management-module Web interface session.

If your BladeCenter unit has a standby management module, the configuration settings of the primary management module are automatically transferred to the second management module. This transfer can take up to 45 minutes.

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 that are 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 following protocols:
  - Lightweight Directory Access Protocol (LDAP)
  - Secure Shell (SSH)
  - Server Service Location Protocol (SLP)
  - Simple Mail Transfer Protocol (SMTP)
  - Simple Network Management Protocol (SNMP)
  - TCP command mode protocol
  - Telnet protocol
- Settings for Secure Sockets Layer (SSL) and Secure Shell (SSH) security
- Security settings such as data encryption and account 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 primary management module that is currently active to the standby management module (for BladeCenter units that support redundant management modules)

**Note:** For BladeCenter units with a standby management module, control automatically switches to the standby management module when the primary management module fails.

## General Settings

Select **MM Control** → **General Settings** to enter identifying information, such as time, date, and location.

The following illustration shows the General Settings page.

[View Configuration Summary](#)

**MM Information** ⓘ

Name:

Contact:

Location:

**MM Date and Time** ⓘ

Date (mm/dd/yyyy): 02/26/2004

Time (hh:mm:ss): 11:32:33

[Set MM Date and Time](#)

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

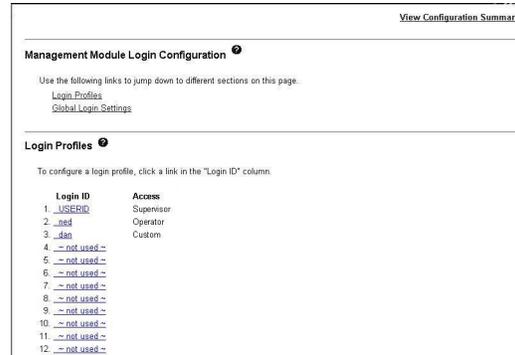
- The name of the management module
- The name of the contact person who is responsible for the management module
- The physical location of the management module
- The real-time clock settings in the management module.
- Enable or disable the trespassing warning and modify warning text. If the warning text is enabled, this message is displayed to users each time that they log in to the management module.

Some of the general settings are used during SNMP and SMTP configuration. See “Configuring SNMP” on page 15 and “Configuring SMTP” on page 18 for additional information.

## Login Profiles

Select **MM Control** → **Login Profiles** to manage user names and permissions.

The following illustration shows login profiles settings.



Up to 12 login profiles can be set up for the management module. Select **Login Profiles** to view information about each login profile. All management-module types display the login ID and role or access level that is assigned to each user: supervisor (S), operator (O), or custom (C).

Click a login ID to configure settings that are specific to a login profile. You also can configure settings that apply to all of the login profiles. The settings for all profiles are configured in the **Global Login Settings** area. Click the login ID of an unused profile to set up a profiles for a new user.

For each user profile, specify the following values:

- Login ID
- Password (requires confirmation)
- Role or Authority Level (default is Operator or Read-Only)  
Defines the command areas that a user can access, according to the user's access scope. Roles or authority levels might vary according to the type of BladeCenter unit that you are using and the management-module firmware version that is installed.
- Access Scope  
Defines where the role or user authority that is defined for a user is valid.

**Important:** Roles or command authority definitions might change between firmware versions. Make sure that the role or command authority level that is set for each user is correct after you update the management-module firmware.

The following illustration shows user profile settings for the newer versions of management-module firmware.

**Login Profile 12** 

Login ID   
Password   
Confirm password

**Role**

- Supervisor (requires Scope selection)
- Operator (readonly, all scopes)
- Custom (requires Roles and Scopes)

**Unassigned roles**

- Chassis operator
- Chassis user account management
- Chassis log administration
- Chassis configuration
- Chassis administration
- Blade operator
- Blade configuration
- Blade administration
- Switch operator
- Switch configuration
- Switch administration

**Assigned roles**

- Blade remote presence

**Access Scope**

**Unassigned**

- Chassis
- Blade 1
- Blade 2
- Blade 3
- Blade 5
- Blade 9
- Blade 10
- Blade 11
- Blade 12
- Blade 14
- Switch 1
- Switch 2
- Switch 3
- Switch 4

**Assigned**

- Blade 4
- Blade 6
- Blade 7
- Blade 8
- Blade 13

[Configure SNMPv3 User](#)

The following illustration shows user profile settings for older versions of management-module firmware.

[View Configuration Summary](#)

---

**Login Profile 1**

Login ID

Password

Confirm password

**Authority Level**

Supervisor

Read-Only

Custom

- User Account Management
- 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)
- Networking & Security Configuration
- Advanced Configuration (MM, I/O Modules, Blades)

[Configure SNMPv3 User](#)

Several user roles (authority levels) are available, and each one gives a user write and execute access to different areas of management-module and BladeCenter component function. Users with operator authority have read-only authority and can access management-module functions for viewing only. Multiple roles can be assigned to each user through the Custom role, and users with the Supervisor role have write and execute access to all functions within their assigned access scopes.

**Attention:** If you change the default login profile on the 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 call for service.

Click **Configure SNMPv3 User** to perform additional user configuration that is required for SNMPv3 (see “Configuring SNMP” on page 15 for instructions).

The following illustration shows the **Global Login Settings** area. The following settings can be modified:

- User authentication method (local, LDAP, or both)
- Lockout period after five unsuccessful login attempts
- Minimum password change interval

---

**Global Login Settings**

These settings apply to all login profiles.

User authentication method

Lockout period after 5 login failures  minutes

---

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

## Alerts

Select **MM Control** → **Alerts** to manage the process of notifying remote users about specified events in the BladeCenter system.

### Management Module Alerts Configuration <sup>?</sup>

Use the following links to jump down to different sections on this page.

- [Remote Alert Recipients](#)
- [Global Remote Alert Settings](#)
- [Monitored Alerts](#)

---

### Remote Alert Recipients <sup>?</sup>

To configure a remote alert recipient, click a link in the "Name" column.

Name	Notification Method	Status
1. <a href="#">Administrator</a>	SNMP over LAN	Receives all alerts
2. <a href="#">Mail Admin</a>	E-mail over LAN	Disabled
3. <a href="#">~ not used ~</a>		
4. <a href="#">~ not used ~</a>		
5. <a href="#">~ not used ~</a>		
6. <a href="#">~ not used ~</a>		
7. <a href="#">~ not used ~</a>		
8. <a href="#">~ not used ~</a>		
9. <a href="#">~ not used ~</a>		
10. <a href="#">~ not used ~</a>		
11. <a href="#">~ not used ~</a>		
12. <a href="#">~ not used ~</a>		

Use **MM Control** → **Alerts** page to perform the following tasks:

- Define remote alert recipients
- Define global remote alert settings
- Define monitored alerts

Select **Remote Alert Recipients** to view a list of all users who must be notified about system events. Click a user name to display a secondary page where you can specify which event notifications are sent, how they are sent (SNMP, e-mail, or IBM Director), where they are sent (e-mail address), and whether the recipient currently is allowed to receive notifications. Click **Generate Test Alert** to make sure that the remote alert recipients will receive the alerts.

Select **Global Remote Alert Settings** to specify how many times the system attempts to send an alert, how long a delay is observed between retries, and whether to include the event log with the notification.

### Global Remote Alert Settings <sup>?</sup>

These settings apply to all remote alert recipients.

Remote alert retry limit  times

Delay between retries  minutes

Include event log with e-mail alerts

Select **Monitored Alerts** to specify which events (from lists of critical, warning, and system alerts) are monitored, and other alert parameters. The specific alerts

that you select apply to all configured alert recipients. If the alert is recoverable, an informational alert is sent in the same category to indicate that a recovery has occurred.

The following illustration shows a Monitored Alerts page.

---

## Monitored Alerts

Use enhanced alert categories

Select the alerts that will be sent to remote alert recipients.

### Critical Alerts

- Select all critical alerts
  - Hard disk drive
  - Multiple Chassis Cooling Device (Blower) failure
  - Power failure
  - Temperature
  - Voltage
  - VRM failure
  - Multiple I/O Module failure
  - Invalid configuration

### Warning Alerts

- Select all warning alerts
  - Single Chassis Cooling Device (Blower) failure
  - Temperature
  - Voltage
  - KVM/media tray switching failure

The following table shows how the legacy and enhanced alert categories map to each other.

*Table 3. Legacy and enhanced alert categories*

Legacy alert categories	Enhanced alert categories
Temperature	Blade servers, I/O modules, and chassis/systems management, as applicable
Voltage	Blade servers, I/O modules, and chassis/systems management, as applicable
Hard disk drive	Blade servers
VRM failure	Blade servers

Table 3. Legacy and enhanced alert categories (continued)

Legacy alert categories	Enhanced alert categories
Multiple chassis cooling device failure (blower)	Cooling devices
Single chassis cooling device failure (blower)	Cooling devices
Power failure	Power modules
Power on	Power on/off
Power off	Power on/off
Multiple I/O module failures	I/O modules
Invalid configuration	I/O modules
KVM/media tray switching failure	Chassis/systems management
Blade throttle	Chassis/systems management
Power management	Chassis/systems management
Event log 100% full	Event log
Event log 75% full	Event log
PFA	Moved to applicable warning
Redundant module failure	Moved to applicable warning
Inventory	Inventory change
Remote login	User activity
Network change	Network change

## Port Assignments

Select **MM Control** → **Port Assignments** to assign I/O ports to various protocols.

The following illustration shows port assignment settings.

[View Configuration Summary](#)

---

**Port Assignments** ⓘ

Currently, the following ports are open on this MM:

23, 6090, 5900, 1044, 1045, 80, 427, 161

You can change the port number for the following services/protocols. You have to restart the MM for the new settings to take effect. Note that you cannot configure a port to a number that is already in use.

HTTP	<input type="text" value="80"/>
HTTPS	<input type="text" value="443"/>
Telnet	<input type="text" value="23"/>
SSH	<input type="text" value="22"/>
SNMP Agent	<input type="text" value="161"/>
SNMP Traps	<input type="text" value="162"/>

Select **Port Assignments** to configure some of the ports that are used by the management module. Management-module ports that can be configured on the Port Assignments page are listed in Table 4 on page 85. Fixed ports that are used by the management module are listed in Table 5 on page 85. Some ports can be modified by only some management-module types.

Table 4. User-configurable management-module ports

Port name	Default port number	Purpose
HTTP	80	Web server HTTP connection using UDP
HTTPS	443	SSL connection using TCP
Telnet	23	Telnet command-line interface connection
SSH	22	Secure Shell (SSH) command-line interface connection
SNMP agent	161	SNMP get/set commands using UDP
SNMP traps	162	SNMP traps using UDP

Table 5. Fixed management-module ports

Port number (fixed)	Purpose
25	TCP e-mail alerts
53	UDP Domain Name Server (DNS) resolver
68	DHCP client connection using UDP
427	UDP Service Location Protocol (SLP) connection
1044	Remote disk function
1045	Persistent remote disk-on-card
5900	Remote control
6090	IBM Director commands using TCP/IP
13991	IBM Director alerts using UDP

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

### Network Interfaces

Select **MM Control** → **Network Interfaces** to configure network access.

The following illustration shows the Network Interfaces page.

[View Configuration Summary](#)

---

**Management Module Network Interfaces** ?

Use the following links to jump down to different sections on this page.

[External Network Interface \(eth0\)](#)  
[Internal Network Interface \(eth1\)](#)  
[TCP Log](#)

---

**External Network Interface (eth0)** ?

Interface: Enabled  
 DHCP: Disabled - Use static IP configuration

\*\*\* Currently the static IP configuration is active for this interface.  
 \*\*\* This static configuration is shown below.

Hostname: MM00096BCA32E0

**Static IP Configuration**

IP address: 160.0.0.31  
 Subnet mask: 255.255.0.0  
 Gateway address: 0.0.0.0

[Advanced Ethernet Setup](#)      [IP Configuration Assigned by DHCP Server](#)

Select **Network Interfaces** to configure the management-module Ethernet interfaces and view the TCP log. For all other management-module types, you can configure both the external Ethernet interface and the internal Ethernet interface that is used for communication with the I/O modules.

For I/O-module communication with a remote management station, 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.

- The **Internal Network Interface (eth1)** section displays information about the interface that communicates with the I/O modules, such as an Ethernet I/O module or the Fibre Channel I/O module. Use it to perform the following tasks:
  - Specify the IP address to use for this interface. The internal network interface (eth1) and the external network interface (eth0) must be on the same subnet.
  - Click **Advanced Ethernet Setup** to 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.
- The **TCP log** section displays entries that are currently stored in the management-module TCP log. This log contains error and warning messages that are generated by the TCP/IP code that is running on the management module; it might be used by a service representative for advanced troubleshooting. The log displays the most recent entries first.  
 You can sort and filter entries in the event log.

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

## Network Protocols

Select **MM Control** → **Network Protocols** to view or change the settings for standard network protocols.

The network protocols settings are similar to the following illustration.

## Management Module Network Protocols <sup>?</sup>

Use the following links to jump down to different sections on this page.

- [Domain Name System \(DNS\)](#)
- [Lightweight Directory Access Protocol \(LDAP\)](#)
- [Remote Control](#)
- [Secure Shell \(SSH\) Server](#)
- [Service Location Protocol \(SLP\)](#)
- [Simple Mail Transfer Protocol \(SMTP\)](#)
- [Simple Network Management Protocol \(SNMP\)](#)
- [SSL Client Configuration for LDAP Client](#)
- [SSL Server Configuration for Web Server](#)
- [TCP Command Mode Protocol](#)
- [Telnet Protocol](#)
- [Web Access \(HTTP/HTTPS\)](#)

Select **Network Protocols** to view or change the settings for SNMP, DNS, SMTP, LDAP, and SLP. You can enable or disable and set the timeout intervals for the Telnet and TCP interfaces.

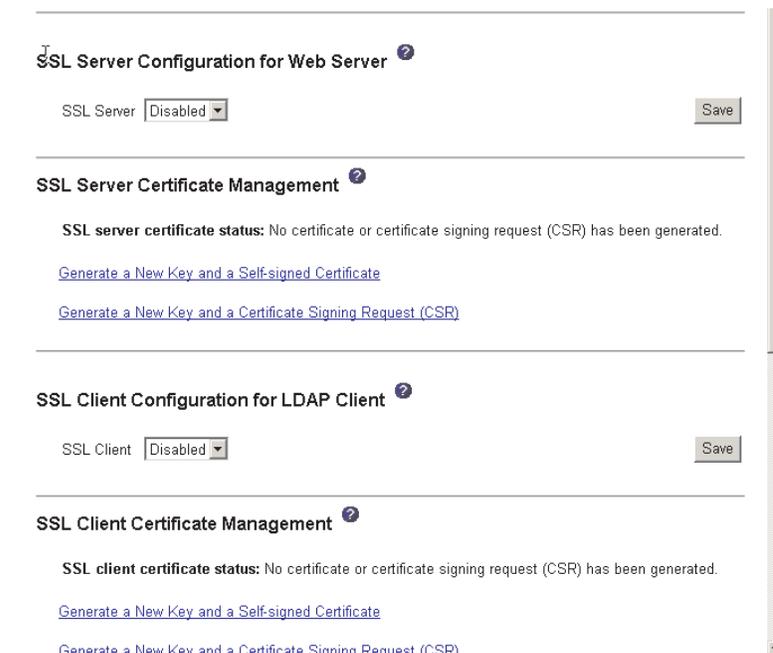
Click **View Configuration Summary** to display the configuration settings for all BladeCenter users and components.

Some of the network protocol settings are used during SNMP, SMTP, and LDAP configuration. See “Configuring SNMP” on page 15, “Configuring SMTP” on page 18, and “Configuring LDAP” on page 19 for additional information.

## Security

Select **MM Control** → **Security** to view and manage security settings.

The following illustration shows security settings.



Select **Security** to view or change the Secure Sockets Layer (SSL) settings for the Web server and LDAP client and to view or change the Secure Shell (SSH) server

settings. You can enable or disable (the default) SSL and select between self-signed certificates and certificates that are provided by a certificate authority (CA). You can also enable (the default) or disable SSH and generate and manage the SSH server key.

The following illustration shows the Secure Shell configuration page.

**Secure Shell (SSH) Server** ?

SSH Server

---

**SSH Server Key Management** ?

SSH server key status: SSH Server key is not installed.

Some of the security settings are used during SSL, LDAP, and SSH configuration. See “Secure Web server and secure LDAP” on page 28 and “Configuring the Secure Shell (SSH) server” on page 38 for additional information.

## Configuration File

Select **MM Control** → **Configuration File** to back up or restore the management-module configuration file.

**Backup MM Configuration** ?

To backup the configuration, click "Backup." You can [view the current configuration summary](#) before backing it up.

---

**Restore MM Configuration** ?

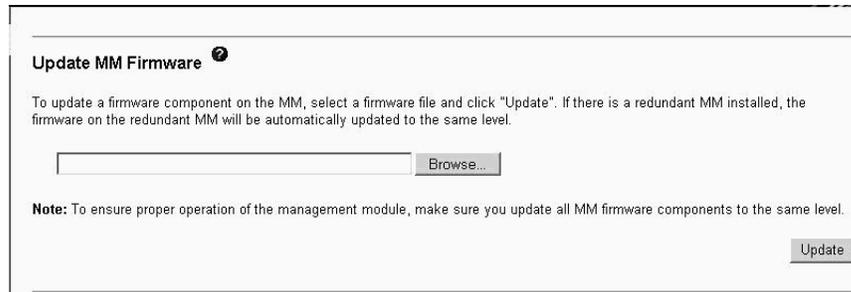
To restore the MM configuration, select a file and click "Restore." To modify the configuration and then restore it, select a file and click "Modify & Restore."

Select configuration file to restore

See “Using the configuration file” on page 42 for instructions.

## Firmware Update

Select **MM Control** → **Firmware Update** to update the management-module firmware.



If a standby management module is installed, the firmware update is automatically applied to both management modules. Click **Browse** to locate the firmware file that you want; then, click **Update**.

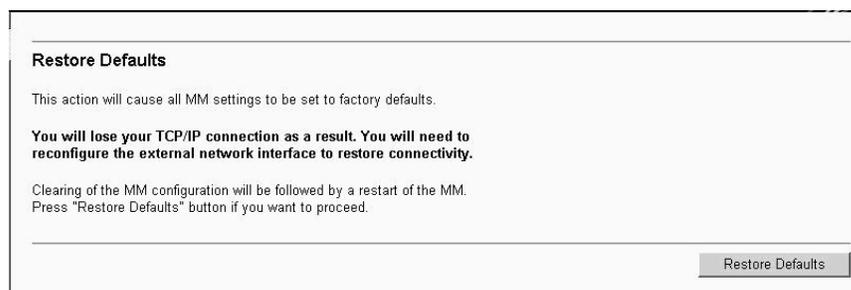
Management-module firmware is in several separate files that are installed independently; you must install all of the firmware update files. You can obtain the firmware files from <http://www.ibm.com/systems/support/>.

**Important:** Make sure that the role or command authority level that is set for each user is correct after you update the management-module firmware, because these definitions might change between firmware versions.

If a standby management module is installed in a BladeCenter unit that previously had only one management module, the firmware in the new management module is updated to the firmware version that is in the primary (already installed) management module. This update takes place when the standby management module is installed. It does not matter whether the new management module contains a later firmware version: the firmware version of the primary management module takes precedence. It can take up to 45 minutes to update the firmware in the standby management module and transfer the management-module configuration.

## Restore Defaults

Select **MM Control** → **Restore Defaults** to restore the factory default configuration of the management module.



Click **Restore Defaults** to close the TCP/IP connections, restart the management module, and reset the configuration to the factory default values.

## Restart MM

Select **MM Control** → **Restart MM** to either restart the management module or to switch control over to an alternate management module in the BladeCenter unit.

The following illustration shows Restart MM page.

---

**Restart MM**

This action will be followed by a restart of the MM. All existing network connections will be temporarily lost as a result. You will need to open a new browser and relogin to get back in to the user interface. Click "Restart" if you want to continue and restart the MM.

---

**Switch Over to Redundant MM**

This action will cause a restart of this MM, followed by a switch over to the redundant MM in bay 2. All existing network connections will be temporarily lost as a result. You will need to open a new browser and relogin to get back in to the user interface. You will also need to move the video, mouse, and keyboard cables to the redundant MM. Click "Switch Over" if you want to continue and switch over to the redundant MM.

**Note:** If you have DHCP enabled on the primary MM's external network interface, and the IP address is assigned by the DHCP server, after the switch over to the redundant MM, the DHCP server will assign a different IP address to the redundant MM. If you want to be able to access both MMs at the same static IP address, you need to disable DHCP. Static IP configuration is the recommended setting in this environment.

---

Select **Restart MM** to restart (reset) the primary management module. If a second management module is installed, you also can select this choice to switch control to the standby management module.

---

## 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 section contains information about where to go for additional information about IBM and IBM products, what to do if you experience a problem with your 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 and any optional devices are 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 *Problem Determination and Service Guide* on the IBM Documentation CD that comes with your system.
- Go to the IBM support Web site at <http://www.ibm.com/systems/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 documentation that is provided with your IBM product. The documentation that comes with IBM systems also describes the diagnostic tests that you can perform. Most systems, operating systems, and programs come with documentation that contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the documentation for the operating system or program.

---

### Using the documentation

Information about your IBM system and preinstalled software, if any, or optional device is available in the documentation that comes with the product. That documentation can include printed documents, online documents, 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/systems/support/> and follow the instructions. Also, some documents are available through the IBM Publications Center at <http://www.ibm.com/shop/publications/order/>.

---

## 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 systems, optional devices, services, and support. The address for IBM System x and xSeries information is <http://www.ibm.com/systems/x/>. The address for IBM BladeCenter information is <http://www.ibm.com/systems/bladecenter/>. The address for IBM IntelliStation<sup>®</sup> information is <http://www.ibm.com/intellistation/>.

You can find service information for IBM systems and optional devices at <http://www.ibm.com/systems/support/>.

---

## Software service and support

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

For more information about Support Line and other IBM services, see <http://www.ibm.com/services/>, or see <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 your IBM reseller or IBM Services. To locate a reseller authorized by IBM to provide warranty service, go to <http://www.ibm.com/partnerworld/> and click **Find a Business Partner** on the right side of the page. For IBM support telephone numbers, see <http://www.ibm.com/planetwide/>. 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.

---

## IBM Taiwan product service

台灣 IBM 產品服務聯絡方式：  
台灣國際商業機器股份有限公司  
台北市松仁路 7 號 3 樓  
電話：0800-016-888

IBM Taiwan product service contact information:

IBM Taiwan Corporation  
3F, No 7, Song Ren Rd.  
Taipei, Taiwan  
Telephone: 0800-016-888

---

## 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.

---

## Trademarks

IBM, the IBM logo, and [ibm.com](http://ibm.com)<sup>®</sup> are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (<sup>®</sup> or <sup>™</sup>), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common

law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at <http://www.ibm.com/legal/copytrade.shtml>.

Adobe and PostScript are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc., in the United States, other countries, or both and is used under license therefrom.

Intel, Intel Xeon, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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

Linux is a registered trademark of Linus Torvalds 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.

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 or DVD drive speed is the variable read rate. Actual speeds vary and are often less than the possible maximum.

When referring to processor storage, real and virtual storage, or channel volume, KB stands for 1024 bytes, MB stands for 1 048 576 bytes, and GB stands for 1 073 741 824 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 can 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.



---

# Index

## A

- accessibility features for this product 2
- Admin/Power/Restart page 74
- advanced features
  - configuring 14
- alarm management
  - BladeCenter T 53, 60
- Alerts page 82
- algorithms, encryption 39
- assistance, getting 91
- authentication, LDAP 81
- authority, user 49

## B

- back up management module
  - configuration 42, 43
- blade server
  - firmware update 69
- Blade Tasks
  - Configuration page 69
  - Firmware Update page 69
  - Power/Restart page 66
  - Remote Control page 67
  - Serial Over LAN page 72
- Blade Tasks pages 66
- BladeCenter T
  - alarm management 53, 60
- BladeCenter unit
  - configuring 10
- BSMP
  - Blade System Management Processor 69
  - BSMP 69

## C

- cabling the management module 7
- certificate signing request 31
- component status
  - detailed 53
- configuration
  - back up for management module 42, 43
  - restore for management module 43
- configuration file
  - restoring 42
  - saving 42
- Configuration File page 88
- Configuration page 75
  - Blade Tasks 69
- configure
  - I/O module 46
  - remote access for management module 11
- configure Ethernet ports 12
- configure LDAP
  - management module 19
- configure LDAP client authentication
  - management module 22

- configuring
  - DNS 17
  - LDAP client authentication 22
  - LDAP search attributes 23
  - management module 10
  - secure shell server 38
  - SMTP 18
  - SNMP 15
  - Wake on LAN (Linux) 42
- configuring advanced features 14
- connecting to management module 5
- current users 56

## D

- data encryption 87
- date stamp 52
- default IP address 8
- detailed component status 53
- detailed power information 63
- difficulty communicating with
  - replacement module 42
- direct connection to management module 7
- Director
  - software 13
- disable Telnet 87
- disk drive
  - mount 45
  - unmount 45
- disk image
  - mount 45
  - unmount 45
- DNS 87
- DNS, configuring 17

## E

- encryption algorithms 39
- encryption, data 87
- error log 57
- Ethernet
  - configuring remote connection 11
- Ethernet ports
  - configure 12
- event log 57
- event log in alerts 82
- Event Log page 57
- event log, viewing 57

## F

- firmware update
  - blade server 69
  - I/O module 77
  - management module 89
- Firmware Update page 69, 77, 89
- firmware VPD 65
- Firmware VPD page 65
- fuel gauge 61

- Fuel Gauge page 61

## G

- general information
  - management module 1
  - management module Web interface 1
- General Settings page 78
- generate
  - certificate signing request 31
  - private encryption key 30, 31
  - self-signed certificate 30
- getting help 91

## H

- hardware requirements
  - Remote Control 6
- hardware service and support
  - IBM reseller 92
  - IBM Services 92
  - telephone numbers 92
- hardware VPD 64
  - modify 64
- Hardware VPD page 64
- help 52
- help, getting 91

## I

- I/O module
  - configure 46
  - firmware update 77
- I/O Module Tasks
  - Admin/Power/Restart page 74
  - Configuration page 75
  - Firmware Update page 77
- I/O Module Tasks pages 73
- IBM Director 13
- IBM Support Line 92
- IP address, default 8
- IP reset button 42
- IP session, set for I/O module 46

## L

- LDAP 87
  - configure (management module) 19
  - configure management module client authentication 22
  - configuring 19
  - configuring client authentication 22
  - configuring search attributes 23
  - overview 19
  - setting up client 19
  - setting up management module client 19
- LDAP authentication 81

- LEDs
  - set color 60
- LEDs page 58
- LEDs page (BladeCenter) 58
- Linux
  - Wake on LAN 42
  - WOL 42
- logged in users 56
- Login Profiles page 79

## M

- management module 5
  - back up configuration 43
  - cabling 7
  - configure LDAP 19
  - configure LDAP client
    - authentication 22
  - connecting to 5
  - default IP address 8
  - direct Ethernet connection 7
  - firmware update 89
  - general information 1
  - network and security
    - configuration 15
  - network connection 7
  - redundant
    - manual changeover 90
  - remote access 11
  - setting up LDAP client 19
- management module configuration 10
  - restore 43
- management module connection
  - overview 6
- management module Web interface
  - general information 1
- management-module Web interface
  - starting 8
- managing alarms
  - BladeCenter T 53, 60
- managing power 61
- MM Control
  - Alerts page 82
  - Configuration File page 88
  - Firmware Update page 89
  - General Settings page 78
  - Login Profiles page 79
  - Network Interfaces page 85
  - Network Protocols page 86
  - Port Assignments page 84
  - Restart MM page 89
  - Restore Defaults page 89
  - Security page 87
- MM Control pages 77
- modify
  - hardware VPD 64
- Monitors
  - Event Log page 57
  - Firmware VPD page 65
  - Fuel Gauge page 61
  - Hardware VPD page 64
  - LEDs page 58
  - LEDs page (BladeCenter) 58
  - System Status page 52
- Monitors pages 52
- mount
  - disk drive 45

- mount (*continued*)
  - disk image 45
- mounting remote drive or image 44

## N

- navigation pane 52
- network and security configuration 15
- network connection to management module 7
- Network Interfaces page 85
- network protocols
  - configuring DNS 17
  - configuring LDAP 19
  - configuring SMTP 18
  - configuring SNMP 15
  - configuring SSL 28
- Network Protocols page 86
- notes, important 94
- notices 3, 93

## O

- overview
  - connecting to management module 6
  - Web interface 49

## P

- port assignments 84
- Port Assignments page 84
- ports 84
- power information
  - detailed 63
- power management 61
- Power/Restart page 66
- private encryption key 30, 31
- protocols
  - DNS 17
  - SMTP 18
  - SNMP 15
  - SSL 28

## R

- related documentation 2
- remote access
  - management module 11
- remote control 67
- Remote Control
  - hardware requirements 6
- Remote Control page 67
- remote disk 44, 68
- replacement module, difficulty
  - communicating with 42
- requirements
  - software 6
- Restart MM page 89
- Restore Defaults page 89
- restore management module
  - configuration 43
- restoring configuration file 42

## S

- saving configuration file 42
- Secure Shell connection clients 39
- secure shell server
  - disabling 39
  - enabling 39
  - generating private key 39
  - overview 38
- Secure Shell server
  - using 40
- secure Web server and secure LDAP
  - configuring security 28
  - enabling SSL for LDAP client 38
  - enabling SSL for secure Web server 35
  - overview 28
  - SSL certificate overview 29
  - SSL client certificate management 36
  - SSL client trusted certificate
    - management 36
  - SSL server certificate management 30
- security 87
- Security page 87
- security, configuring 28
- self-signed certificate 30
- serial over LAN 72
- Serial Over LAN page 72
- setting up LDAP client 19
  - management module 19
- SLP 87
- SMTP 87
- SMTP, configuring 18
- SNMP 87
- SNMP, configuring 15
- software requirements 6
- software service and support 92
- SOL 72
- SSH 87
  - disabling 39
  - enabling 39
- SSH clients 39
- SSL certificate overview 29
- SSL client certificate management 36
- SSL client trusted certificate
  - management 36
- SSL security protocol 28
- SSL server certificate management 30
- SSL, enabling
  - for LDAP client 38
  - for secure Web server 35
- SSL, LDAP 87
- starting the management-module Web interface 8
- statements 3
- support, web site 91
- System Status page 52

## T

- TCP 87
- TCP log 86
- TCP log, viewing 86
- telephone numbers
  - hardware service and support 92
- Telnet, disable 87
- time stamp 52

trademarks 93

## U

unmount

disk drive 45

disk image 45

user authority 49

user roles 49

users, logged in 56

using

Secure Shell server 40

## V

vital product data

firmware 65

hardware 64

VPD

firmware 65

hardware 64

## W

Wake on LAN

configuration 40

Linux configuration 42

verify configuration 41

WOL 40, 41

Web browsers, supported 6

Web interface

management module 5

Web interface overview 49

Web interface pages

user authority required 49

web site

publication ordering 91

support 91

support line, telephone numbers 92

Web site

BladeCenter Planning and Installation  
Guide 3

WOL

configuration 40

verify configuration 41

Wake on LAN 40, 41







Part Number: 44R5370

Printed in USA

(1P) P/N: 44R5370

