BladeCenter Advanced Management Module
BladeCenter T Advanced Management Module

User's Guide

BladeCenter Advanced Management Module
BladeCenter T Advanced Management Module

User's Guide

Note: Before using this information and the product it supports, read the general information in "Getting help and technical assistance," on page 193, "Notices" on page 197, the *Warranty Information* document, and the *Safety Information* and *Environmental Notices and User Guide* documents on the IBM *Documentation* CD.

Twenty-sixth Edition (March 2012)

Contents

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 management modules other than the advanced management module is in a separate document.

Although all types of management modules have similar functions, 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.

- When a command is labeled "(BladeCenter H only)," it can run on all types of BladeCenter H units (BladeCenter H and BladeCenter HT).
- When a command is labeled "(BladeCenter T only)," it can run on all types of BladeCenter T units (BladeCenter T and BladeCenter HT).

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).

Note: The advanced management module has two USB ports. If you install a USB storage device in one of the ports, blade servers in the BladeCenter unit also can use this storage device. The rules that determine which blade server detects the USB storage device are as follows:

1. For the BladeCenter unit and BladeCenter T unit, the USB storage device mounts to the blade server that has ownership of the KVM.
2. For the BladeCenter H or HT unit, the USB storage device mounts to the blade server that has ownership of the media tray.

You configure BladeCenter components by using the management module, setting parameters or values 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.

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 that appears 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 Advanced Management Module Command-Line Interface Reference Guide*

  This document explains how to use the management-module command-line interface (CLI) 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.

- *BladeCenter Advanced Management Module Messages Guide*

  This document provides additional information about event notifications from the advanced management module or messages in the advanced management module event log and the steps that you can take to resolve issues on a BladeCenter chassis.
- *IBM SMASH Proxy Installation and User's Guide*

  This document provides an overview of the Systems Management Architecture for Server Hardware (SMASH) command-line protocol (CLP) standard; its history, features, and components; and its relationship to the IBM SMASH product. This document also provides a detailed overview of SMASH Proxy and SMASH Embedded, including configuration, functionality, accessibility, features, and components.
- *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/.

IBM Redbooks publications are developed and published by the IBM International Technical Support Organization (ITSO). The ITSO develops and delivers skills, technical know-how, and materials to IBM technical professionals, Business Partners, clients, and the marketplace in general. For IBM Redbooks publications for your BladeCenter, go to http://www.redbooks.ibm.com/portals/bladecenter.

To obtain license keys for features that you have purchased for your BladeCenter unit, go to http://licensing.datacentertech.net.

Notices and statements in this document

Notices and statements are used in this document to focus extra attention on information.

The caution and danger statements in this document 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 document:

- **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

The following topics describe the techniques for connecting to, starting, configuring, and using the management-module web interface.

- "Connecting to the management module"
- "Starting the management-module web interface" on page 11
- "Configuring the management module" on page 13
- "Communicating with the IBM Systems Director software" on page 22
- "Advanced features" on page 23
- "Configuring an I/O module" on page 82

See Chapter 3, "Management-module web interface overview," on page 87 for a detailed description of the structure and content of the management-module web interface. You also can perform web interface functions through the management-module command-line interface (CLI) and by using the SMASH command-line protocol standard. See the *BladeCenter Management Module Command-Line Interface Reference Guide* and the *IBM SMASH Proxy Installation and User's 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. The advanced management module also supports CLI-only connection through the serial management port.

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. You can also access the command-line interface by using a Secure Shell (SSH) server or the advanced management module serial port. 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:

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 11 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 medium access control (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, you need 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, you can use either a standard Ethernet cable or an Ethernet crossover cable.

Connections through the advanced management-module serial port can access only the management-module CLI. For information about accessing the management-module CLI, see the *BladeCenter Advanced Management Module Command-Line Interface Reference Guide*.

Hardware requirements

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

- Microprocessor: Intel Pentium III or later, operating at 700 MHz or faster (or equivalent)
- Memory: 256 MB RAM
- Video: 16 MB 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	70 Hz
1024 x 768	75 Hz

Software requirements

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

- Microsoft Internet Explorer 6.0 or later (with the latest Service Pack installed)
- Mozilla Firefox version 1.07 or later

Note: The I/O Module web interface is supported only by Mozilla Firefox version 1.07 or later.

The remote console (remote control) is supported by Java Runtime Environment (JRE) version 6.0, update 10 or later, available at http://www.java.com/. The Java Virtual Machine (JVM) Plug-in is part of the JRE. The JRE and JVM versions installed on a client computer must match: make sure that no other versions of JRE or JVM are installed.

The following are the minimum server operating systems levels that support USB, which is required for the Remote Control feature:

- Microsoft Windows Server 2003
- Microsoft Windows 2000 with Service Pack 4
- 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 and information. See the *BladeCenter Advanced 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 9.

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 cable or 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.

Note: The advanced management module can perform an automatic media dependent interface (MDI) crossover, eliminating the need for crossover cables or cross-wired (MDIX) ports. You might have to use a crossover cable to connect to the advanced management module if the network interface card in the client computer is very old.

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.

Note: The advanced management module does not have a fixed static IPv6 IP address by default. For initial access to the advanced management module in an IPv6 environment, users can either use the IPv4 IP address or the IPv6 link-local address. See "IPv6 addressing for initial connection" on page 10 for information about how to determine the IPv6 address to use for initial advanced management module access.

The management module has the following default network settings:

- IPv4 IP address: 192.168.70.125 (primary and secondary management module)
- IPv4 Subnet: 255.255.255.0
- User ID: USERID (all capital letters)
- Password: PASSW0RD (note the number zero, not the letter O, in PASSW0RD)

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. For IPv4 connection, make sure that the subnet of the client computer is set to the same value as the default management module subnet (listed above).
2. Open a web browser on the client computer, and direct it to the default management-module IP address (listed above).
3. Enter the default user name, USERID, and the default password, PASSW0RD, 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 13).

IPv6 addressing for initial connection

When using IPv6 addressing, the only way to initially connect to the advanced management module is by using the IPv6 link-local address.

The link-local address is a unique IPv6 address for the advanced management module that is automatically generated based on its MAC address. It is of the form: `FE80::3BA7:94FF:FE07:CBD0`.

The link-local address for the advanced management module can be determined in one of the following ways:

- Some advanced management modules will list the link-local address on a label that is attached to the advanced management module.
- If you are able to log in to the management module command-line interface (CLI) using IPv4 addressing, the link-local address can be viewed using the `ifconfig` command (see the *BladeCenter Advanced Management Module Command-Line Interface Reference Guide* for information for information).
- If you are able to log in to the management module web interface using IPv4 addressing, the link-local address can be viewed in the Primary Management Module, IPv6 section of the **MM Control → Network Interfaces** page (see "Network Interfaces" on page 165 for information).

If the advanced management module does not have a label listing the link-local address and you are unable to access the advanced management module using IPv4, complete the following steps to calculate link-local address:

1. Write down the MAC address of the advanced management module. It is on a label on the management module, below the IP reset button. The label reads MM*xxxxxxxxxxxx*, where *xxxxxxxxxxxx* is the MAC address. For example,

   `39-A7-94-07-CB-D0`
2. Split the MAC address into two parts and insert FF-FE in the middle. For example,

   `39-A7-94-`**`FF-FE`**`-07-CB-D0`
3. Convert the two hexadecimal digits at the left end of the string to binary. For example,
   - **`39`**`-A7-94-FF-FE-07-CB-D0`
   - **`00111001`**`-A7-94-FF-FE-07-CB-D0`
4. Invert the value for bit 7 of the binary string. For example,
   - `00111`**`0`**`1-A7-94-FF-FE-07-CB-D0`
   - `00111`**`1`**`1-A7-94-FF-FE-07-CB-D0`
5. Convert the binary digits at the left end of the string back to hexadecimal. For example,
   - **`00111011`**`-A7-94-FF-FE-07-CB-D0`
   - **`3B`**`-A7-94-FF-FE-07-CB-D0`
6. Combine the hexadecimal digit pairs into 4-digit groups. For example,
   - `3B-A7-94-FF-FE-07-CB-D0`
   - `3BA7-94FF-FE07-CBD0`
7. Replace dash (-) separators with colon (:) separators. For example,
   - `3BA7-94FF-FE07-CBD0`
   - `3BA7:94FF:FE07:CBD0`
8. Add FE80:: to the left of the string. For example,

   `FE80::``3BA7:94FF:FE07:CBD0`

For a MAC address of 39-A7-94-07-CB-D0, the link-local address used for initial IPv6 access is FE80::3BA7:94FF:FE07:CBD0.

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 6.0 or later (with the latest Service Pack installed)
- Mozilla Firefox version 1.07 or later

Note: The I/O Module web interface is supported only by 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. (For details, see the *Installation Guide* for your management module.)

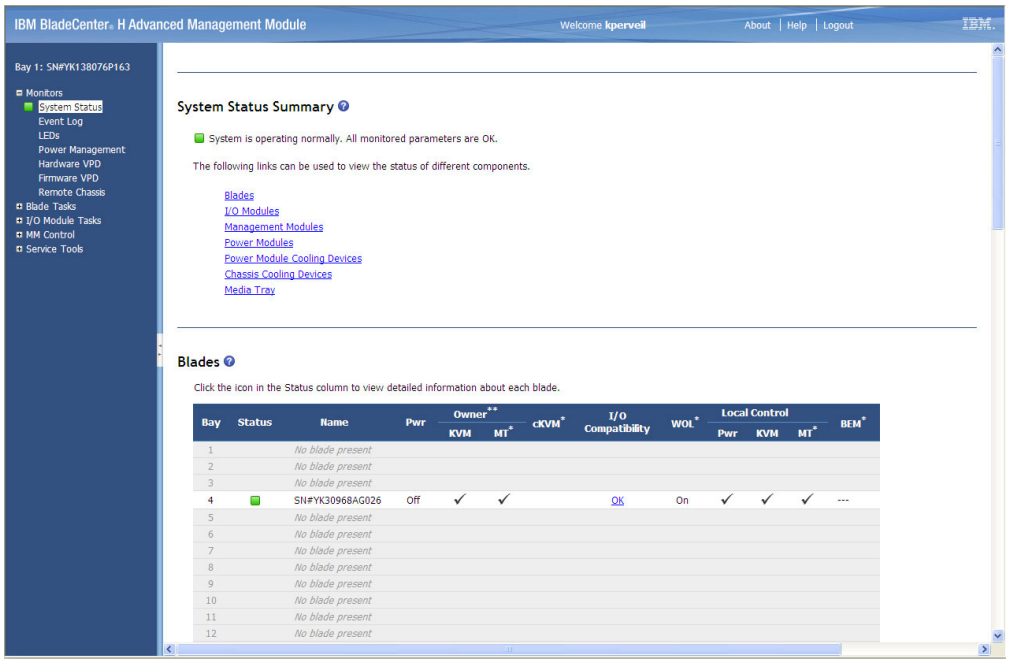
   Note: The factory-defined static IPv4 IP address is 192.168.70.125, the default IPv4 subnet address is 255.255.255.0, and the default host name is MM*xxxxxxxxxxx*, where *xxxxxxxxxxx* is the burned-in MAC address. The MAC address is on a label on the management module, below the IP reset button. See "IPv6 addressing for initial connection" on page 10 for information about how to determine the IPv6 address to use for initial advanced management module access.

   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: PASSW0RD (note the zero, not O, in PASSW0RD)
3. Follow the instructions on the screen. Be sure to set the timeout value that you want for your web session. If you select the **Use automatic refresh** check box, some pages can have their data automatically refreshed.

Note: The first time you start the management module after a firmware update, a page displays that shows information about licensed features that are active. Information about active and inactive licensed features is in the **MM Control → Licensed Features** page (see "License Manager" on page 181 for information).

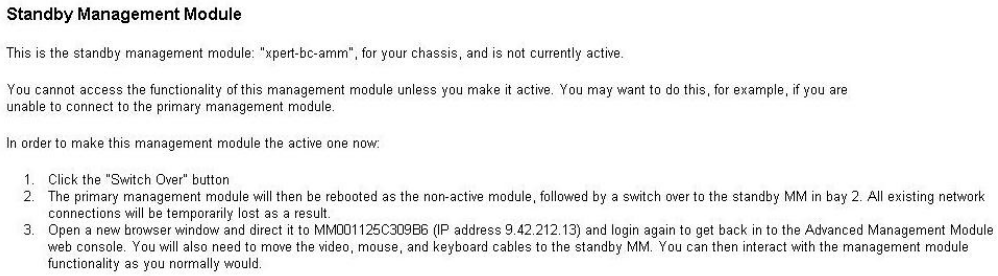
The BladeCenter management-module web-interface page opens. The content of this page and all other web-interface pages varies according to the type of BladeCenter unit that you are using and the firmware versions and options that are installed. See Chapter 3, "Management-module web interface overview," on page 87 for detailed information about the management-module web interface.



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 management modules other than 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.

For advanced management modules, you can start a web-interface session with the standby management module, if the network interface for the standby management module has been configured. No function is provided by the standby interface, beyond initiating a failover from the primary management module.



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.

For advanced management modules, you can manually set the network configuration of the standby management module as part of advanced failover, making it accessible if there is a problem during automated failover. 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 67 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 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. For additional information, see the documentation that comes with each I/O module.

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 165). 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 165). Internal Ethernet ports for the advanced management module cannot be manually configured.
- The management port on each I/O module that 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 141).

  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.

Note: Do not configure the blade server and the AMM to be on the same IP subnet. The AMM should be on an IP subnet dedicated to management traffic.

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

For IPv4, you can configure the management module to use Dynamic Host Configuration Protocol (DHCP) or static IP addresses for remote access. For IPv6, you can configure the management module to use Dynamic Host Configuration Protocol (DHCPv6), static IP addresses, and stateless auto-configuration 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:

- For IPv4:
  - If you have an accessible, active, and configured dynamic host configuration protocol (DHCP) server on the network, the IP address, gateway address, subnet mask, and DNS server IP addresses (IPv4) 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 configuration information until after this period passes.
- For IPv6:
  - If there is an accessible and active IPv6 router on the network, the advanced management module will generate stateless auto-configured addresses for the Ethernet ports.
  - If there is an accessible, active, and configured DHCPv6 server on the network, the advanced management module will also receive a DHCPv6-assigned IP configuration.
  - The link-local IPv6 address is always available for use when IPv6 is enabled. See "IPv6 addressing for initial connection" on page 10 for information about how to determine the link-local address.

Any 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 11 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 IPv4 IP address is 192.168.70.125, the default IPv4 subnet address is 255.255.255.0, and the default host name is MM*xxxxxxxxxxx*, where *xxxxxxxxxxx* is the burned-in MAC address. The MAC address is on a label on the management module, below the IP reset button. See "IPv6 addressing for initial connection" on page 10 for information about how to determine the IPv6 address to use for initial advanced management module access.

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 port

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

Note: Do not configure the blade server and the AMM to be on the same IP subnet. The AMM should be on an IP subnet dedicated to management traffic.

To configure the management-module external Ethernet port, complete the following steps:

1. Under **MM Control** in the navigation pane, click **Network Interfaces**.

   Attention: Once IPv6 has been enabled, disabling it or updating advanced management module firmware to a level that does not support IPv6 addressing causes all IPv6 connectivity to be lost. Services and interfaces that are configured for IPv6 operation might not function properly and you will need to reconfigure these services and interfaces.
2. In the **External Network Interface (eth0)** section, enable or disable IPv6 addressing using the **IPv6 Enabled** checkbox. IPv4 addressing is always enabled and IPv6 is enabled by default. If IPv6 addressing is disabled for the BladeCenter unit, you will see an additional checkbox to suppress display of IPv6 information. You must click **Save** for any changes to take effect.

   Note: If IPv6 is enabled, at least one of the IPv6 configuration methods (IPv6 static, DHCPv6, or stateless auto-configuration) must also be enabled and configured.
3. Configure the IPv4 and IPv6 external Ethernet interface (eth0) in the **Primary Management Module** section.

   Note: For I/O-module communication with a remote management station, such as a management server that is running IBM Systems 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.

   a. The following configuration settings apply to both IPv4 and IPv6 addressing:
      - **Hostname** field: (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).
      - **Domain name** field: The domain name of the management module that is used in conjunction with a dynamic domain name server (DDNS).
      - **Register this interface with DNS** checkbox: If checked, the configured DNS servers (see "Network Protocols" on page 170) will also be considered DDNS servers and domain name information will be sent to them.

b. The following configuration settings apply to IPv4 addressing:
   - **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)

     Note: If the management-module DHCP setting is set to **Try DHCP server. If it fails, use static IP config.**, the management module uses the static IP address when the DHCP server is not available during management-module startup. When this occurs, the IP address might not be reachable if multiple management modules were started with the same static IP address.
   - **IPv4 Static IP configuration**: Configure this information only if DHCP is disabled.
     - **IP address**: The IPv4 IP address of the management module 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**: The subnet mask must contain four integers from 0 to 255, separated by periods, with no spaces. The default setting is 255.255.255.0
     - **Gateway address**: The IP address of your network gateway router 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 that were specified above.
   - Click **IP Configuration Assigned by DHCP Server** to view the IP configuration that was assigned by the DHCP server. (This choice is available only when DHCP is enabled.)

c. The following configuration settings apply to IPv6 addressing. They will only be seen if IPv6 is enabled or if IPv6 is disabled and display of IPv6 settings has not been suppressed.

   Note: For IPv6, both DHCPv6 and IPv6 static configuration can be enabled at the same time, each with their own address. Hosts like the advanced management module can have multiple IPv6 addresses.
   - **Link-local address**: (read only) A unique IPv6 address for the advanced management module that is automatically generated based on the MAC address.
   - **IPv6 Static IP configuration**: IPv6 static IP configuration is disabled by default.

     Note: The advanced management module will not have a fixed static IPv6 address by default. For initial access, users can use either the default IPv4 address or the IPv6 link-local address.
     - **IP address**: The IPv6 IP address of the management module must be 16 hexadecimal bytes, divided along 2-byte boundaries, delimited with colons, of the form: 2001:0DB8:0000:0000:02AA:00FF:FE28:9C5A
     - **Address prefix length (1-128)**: The prefix length for the IPv6 address. The address prefix length is not configurable for the standby advanced management module: the same value as the primary advanced management module is used.

- **Default route**: The IP address of your network gateway router must be 16 hexadecimal bytes, divided along 2-byte boundaries, delimited with colons, of the form: 2001:0DB8:0000:0000:02AA:00FF:FE28:9C5A. The default route is not configurable for the standby advanced management module: the same value as the primary advanced management module is used.

  - **DHCPv6**: Select one of the following choices:
    - **Enabled: Obtain IP configuration from DHCP server** (the default)
    - **Disabled: Not obtain IP configuration from DHCP server**
  - **Stateless Auto-configuration**: Automatic configuration of addresses is based on the receipt of Router Advertisement messages. These messages include stateless address prefixes. Stateless auto-configuration is enabled by default.

4. 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.
   - Some I/O modules do not support IPv6 addressing.

   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. For IPv4, 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: PASSW0RD (note the zero, not O, in PASSW0RD)

5. 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.

Using the configuration wizard

You can use the advanced management module configuration wizard to configure an advanced management module.

The configuration wizard starts automatically when you access the web interface of a new advanced management module for the first time. The configuration wizard also starts automatically the first time that you access the web interface of an advanced management module that has been reset to its factory default settings.

To use the configuration wizard, click **Configuration Wizard** under **Configuration Mgmt** in the navigation panel. You must be assigned the Supervisor role (command authority) to use the configuration wizard. The configuration wizard supports **Express** and **Custom** paths to configuration.

- The **Express** option preselects a number of common settings.
- The **Custom** option prompts you for the necessary configuration information for each component.

After you select the configuration path, the **Getting Started** page summarizes the information that you will need to complete the configuration process. Click **View Configuration Worksheet** to view and print out a convenient form for collecting this information.

After you gather this information, enter it into the wizard pages to complete a basic configuration of the management module. If you are importing a saved management module configuration or restoring one that is saved to the backplane of the BladeCenter unit, these options are in the **Import Configuration** page of the configuration wizard. Imported or restored configurations do not require any additional information entry.

The completion page has a three radio button selections and a **Finish** button. The radio button selections are:

- **Restart Management Module now to ensure all changes are applied**
- **Allow me to update my Management Module Firmware now**
- **Do none of the above**

Configuring a blade server management network

You can use the web interface to configure the management network for a blade server.

To configure the management network for a blade server, complete the following steps:

1. Under **Blade Tasks** in the navigation pane, click **Configuration**.

   Note:
   - See "Configuring the management-module Ethernet port" on page 16 for information about enabling or disabling IPv6 addressing for your BladeCenter unit.
   - If a blade server supports IPv6 addressing and IPv6 is enabled, both the IPv4 and IPv6 configuration fields are shown. If a blade server does not support IPv6 addressing, or if IPv6 addressing is disabled and you have chosen to hide IPv6 fields when IPv6 addressing is disabled, only the IPv4 configuration fields are shown.
   - If IPv6 addressing is enabled and a blade server supports IPv6 addressing, at least one IPv6 configuration method must be configured.
2. Select the **Management Network** tab.
3. In the **Interface Management** section, click the link for the blade server you want to configure in the **Name** field.
4. Select the tab for the management interface to configure, **eth0** or **eth1**.
5. Configure settings that apply to both IPv4 and IPv6 in the **General Settings** section:
   - **Enable/Disable NIC**: Enables or disables this management network interface. If the interface is disabled, all other configuration items are ignored.
   - **Enable/Disable IPv6**: Enables or disables IPv6 addressing for this management network interface.
   - **VLAN ID**: (Optional) The Virtual LAN (VLAN) ID for this management network interface.
   - **Route traffic through**: (Optional) The device that this management network interface uses for communications.
   - **Mac address** (read only): The MAC address of this network interface for the blade server Blade System Management Processor (BSMP).

6. Configure settings in the **IPv4** section:
   - **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)

     Note: If the DHCP setting is set to **Try DHCP server. If it fails, use static IP config.**, the management network interface uses the static IP address when the DHCP server is not available during startup. When this occurs, the IP address might not be reachable if multiple devices were started with the same static IP address.
   - **IP address**: The IPv4 IP address of the management network interface must contain four integers from 0 through 255, separated by periods, with no spaces or consecutive periods.
   - **Subnet mask**: The subnet mask must contain four integers from 0 to 255, separated by periods, with no spaces.
   - **Gateway address**: The IP address of your network gateway router 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 that were specified above.
7. Configure settings in the **IPv6** section:
   - **Static IP configuration**: Enable or disable static IPv6 addressing for the management network interface. IPv6 static IP configuration is disabled by default.
   - **IP address**: The IPv6 IP address of the management network interface must be 16 hexadecimal bytes, divided along 2-byte boundaries, delimited with colons, of the form: 2001:0DB8:0000:0000:02AA:00FF:FE28:9C5A
   - **Prefix length**: The prefix length for the IPv6 address, between 1 and 128, inclusive.
   - **Default route**: The IP address of your network gateway router must be 16 hexadecimal bytes, divided along 2-byte boundaries, delimited with colons, of the form: 2001:0DB8:0000:0000:02AA:00FF:FE28:9C5A.
   - **Link-local address**: (read only) A unique IPv6 address for the management network interface that is automatically generated based on the MAC address.
   - **DHCPv6**: Select one of the following choices:
     - **Enabled**: Obtain IP configuration from DHCP server (the default).
     - **Disabled**: Do not obtain IP configuration from DHCP server
   - **Stateless Auto-configuration**: Enable or disable stateless auto-configuration for the management network interface. Automatic configuration of addresses is based on the receipt of Router Advertisement messages. These messages include stateless address prefixes. Stateless auto-configuration is enabled by default.
8. Scroll to the bottom of the page and click **Save**.

When the blade server management network configuration is modified, it might take several minutes before the advanced management module can display the new values.

Communicating with the IBM Systems Director software

IBM Systems Director is a platform-management foundation that streamlines the way you manage physical and virtual systems in a heterogeneous environment. By using industry standards, IBM Systems Director supports multiple operating systems and virtualization technologies in IBM and non-IBM x86 platforms.

The IBM Systems Director program is a systems-management product that comes with some BladeCenter units. The IBM Systems Director software communicates with the BladeCenter unit through the Ethernet port on the active management module. For more information about IBM Systems Director, see the documentation on the *IBM Systems Director CD* that comes with the server and the IBM xSeries® Systems Management web page at http://www.ibm.com/systems/management/, which presents an overview of IBM Systems Management and IBM Systems Director. This page also lists the minimum version of IBM Director software that you require 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 Systems Director-enabled server.

To communicate with the BladeCenter unit, the IBM Systems Director software needs a managed object (in the Group Contents page of the IBM Systems 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 Systems Director managed object for the unit. If the IP address is not known, the IBM Systems 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 Systems Director software to discover the BladeCenter unit, your network must initially provide connectivity from the IBM Systems 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 Systems 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 Systems 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.

Advanced features

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

- "Network and security configuration"
- "Configuring Wake on LAN" on page 63
- "Using the configuration file" on page 65
- "Using the remote console feature" on page 69
- "Using the remote disk feature" on page 70
- "Using management channel auto-discovery" on page 72
- "IBM Service Advisor" on page 75

Detailed descriptions of the management-module web interface are in Chapter 3, "Management-module web interface overview," on page 87.

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 27)
- SSL and LDAP (see "Configuring LDAP" on page 27)
- Secure web server and secure LDAP (see "Secure web server and secure LDAP" on page 44)
- SSH (see "Configuring the Secure Shell (SSH) server" on page 56)
- SMASH (see "Enabling SMASH" on page 60)
- Syslog (see "Enabling Syslog" on page 61)
- TFTP on Linux (see "Configuring Linux TFTP server" on page 63)

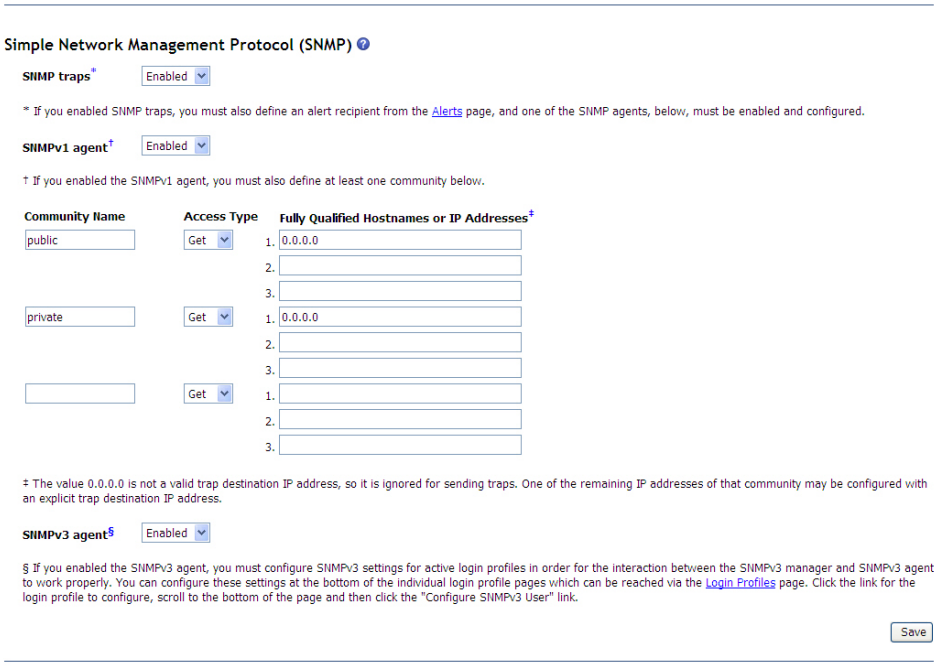
Configuring SNMP

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 11.
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.



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.

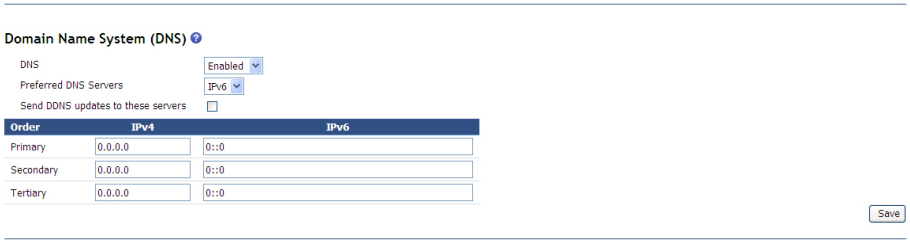
   Note: Alert recipients whose notification method is SNMP will not receive alerts unless both the SNMP agent and the SNMP traps are enabled.
6. If you are enabling the SNMPv1 agent, complete the following steps to set up a community that defines the administrative relationship between SNMP agents and SNMP managers; otherwise, continue with step 7 on page 26. 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 (for IPv4) or 0::0 (for IPv6) 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 steps, 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.



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 and IPv6 addressing is enabled, use the **Preferred DNS Servers** field to select which IP addresses to use first when both IPv6 and IPv4 IP addresses are specified for the DNS servers (IPv6 is the default setting).
10. (Optional) If you enabled DNS, select the **Send DDNS updates to these servers** checkbox to send DNS information to the dynamic domain name servers (DDNS).
11. (Optional) If you enabled DNS, in the **DNS server IP address** fields, specify the IP addresses of up to three DNS servers each for IPv4 and IPv6 on your network.
12. Scroll to the bottom of the page and click **Save**.
13. If you are enabling the SNMPv3 agent, complete the following steps to configure the SNMPv3 profile for each SNMPv3 user; otherwise, configuration is complete.
    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.

    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 13b on page 26 and step 13c on page 26 for each SNMPv3 user.

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 11.
2. In the navigation pane, click **MM Control → Network Protocols**, and scroll down to the **Simple Mail Transfer Protocol (SMTP)** section.

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

Configuring LDAP

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

The advanced management module supports both local and remote user authentication. Local authentication uses information provided in the **MM Control → Login Profiles** page to authenticate users. Using an LDAP server, a management module can authenticate a user by querying or searching an LDAP directory on a remote LDAP server, instead of going through its local user database.

When any type of remote authentication is used, you can choose to have the permissions for each successfully authenticated user authorized either locally or based on information stored on the LDAP server used for remote authentication. The permissions that are authorized for a user specify the actions that each user can perform while logged in to the advanced management module.

The three remote authentication methods are described in the following topics:

- "Active Directory authentication with local authorization" on page 28
- "Active Directory role-based authentication and authorization" on page 31
- "Legacy LDAP authentication and authorization" on page 35

Active Directory authentication with local authorization:

You can set up remote LDAP authentication for users, with local user authorization, using Active Directory.

Note: Active Directory authentication with local authorization applies only to BladeCenter units deployed in an Active Directory environment.

When using Active Directory authentication with local authorization, the Active Directory servers are used only to authenticate users, verifying the credentials for a user. There is no authorization information stored on the Active Directory server for a given user; the advanced management module stored group profiles must be configured with authorization information.

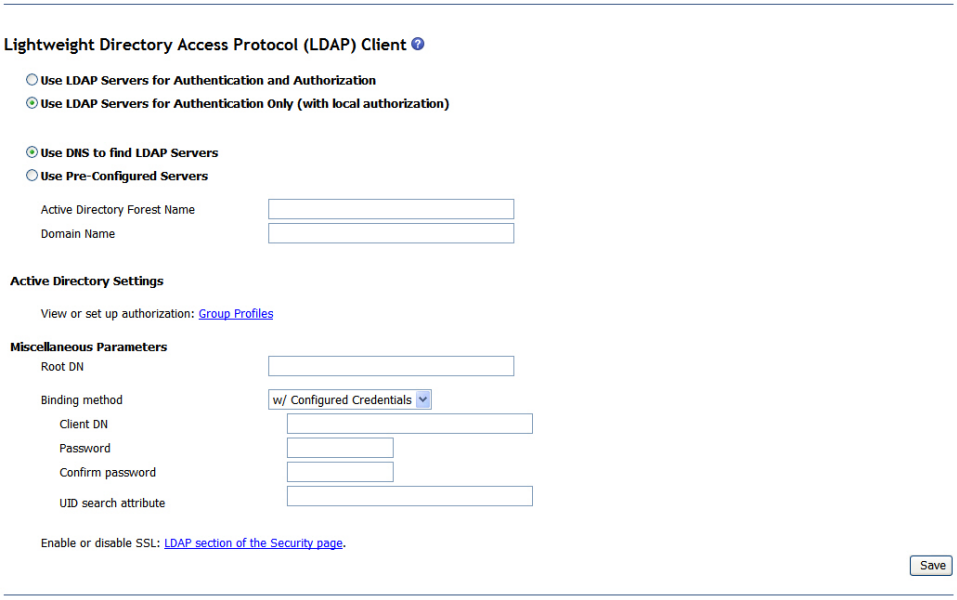
Authorization information used to configure the group profiles can be obtained by retrieving membership information for a user from the Active Directory server. This membership information gives the list of groups to which a user belongs (nested groups are supported). The groups specified on the Active Directory server are then compared to the group names locally configured on the advanced management module. For each group that matches, the user is assigned permissions from that group. That is, for each group name that is locally configured on the advanced management module, there is a corresponding authorization profile that is also configured for that group.

The advanced management module supports up to 16 locally-configured group names. Each group name is limited in length to 63 characters. One of the following attributes must be configured as the group name in order to match the group membership information retrieved from the Active Directory servers:

- Distinguished Name
- "cn" attribute
- "name" attribute
- "sAMAccountName" attribute

To configure Active Directory authentication with local authorization for the advanced management module, complete 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.
3. Select **Use LDAP Servers for Authentication Only (with local authorization)**.
4. The domain controllers (DC) to be used for authentication can either be manually configured or discovered dynamically via DNS SVR records.
   - Select **Use DNS to find LDAP Servers** to dynamically discover the domain controllers based on DNS SVR records (see step 5).
   - Select **Use Pre-Configured LDAP Servers** (default) to manually configure the domain controllers (see step 6 on page 29).
5. If you are using DNS to dynamically discover the domain controllers, configure the following settings; then, go to step 7 on page 30.



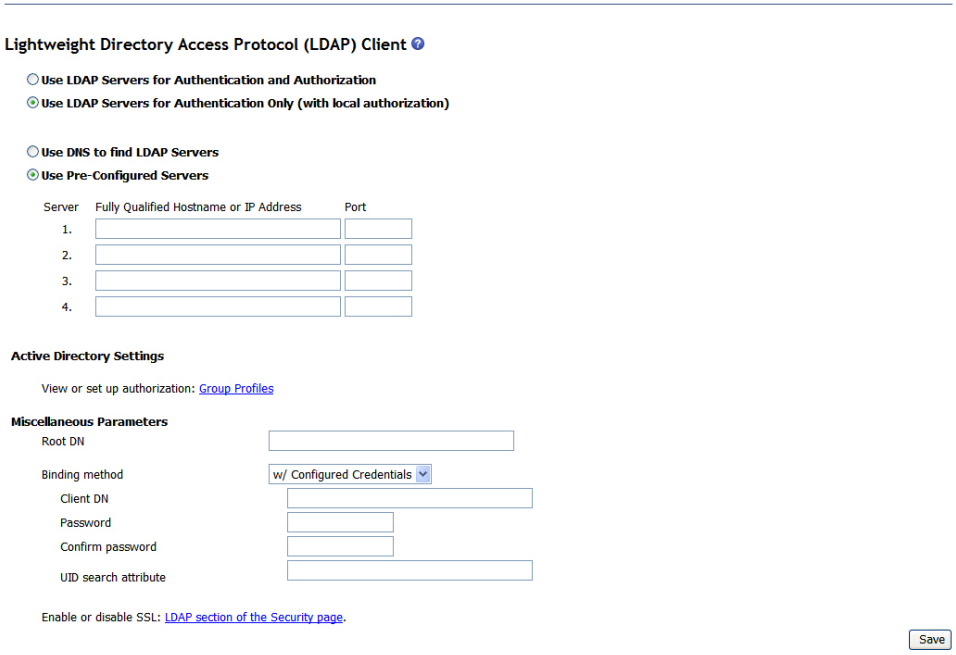
Domain Name

The fully qualified domain name of the domain controller. The domain name is needed to find the domain controller.

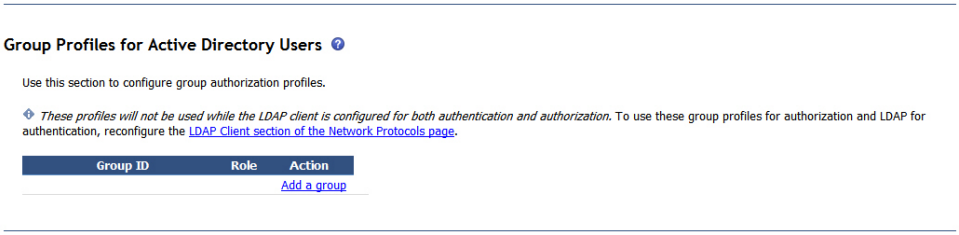
Active Directory Forest Name

This optional parameter is used to discover global catalogs (GC). Global catalogs are required for users who belong to universal groups in cross-domains. In environments where cross-domain group membership does not apply, this field can be left blank.

6. If you are manually configuring the domain controllers and global catalogs, configure the **LDAP Server Host Name or IP Address** and **Port** fields; then, go to step 7 on page 30. Up to four domain controllers can be configured using an IP address or a fully qualified hostname. Global catalog servers are identified using port number 3268 or 3269: any other port number indicates that a domain controller is being configured.



7. If you are using group authorization profiles, view or configured them by clicking **Group Profiles**; then, return to the **MM Control → Network Protocols** page and scroll to the **Lightweight Directory Access Protocol (LDAP) Client** section.



8. Configure the following **Miscellaneous Parameters**:

Root DN

This optional parameter is used to configure the base distinguished name (DN) of the Active Directory server (for example, dn=companyABC,dn=com). In most cases, this field is left blank, although it can be useful for debugging purposes.

The advanced management module normally uses the RootDSE query to find the base distinguished name of an Active Directory server with which it communicates. This base distinguished name is then used for subsequent searches. The base distinguished name is derived from the `defaultNamingContext` and `rootDomaintNamingContext` attributes retrieved from the RootDSE query. When the base distinguished name is set using the **Root DN** field, it overrides the `defaultNamingContext` and `rootDomaintNamingContext` attributes.

Binding Method

For initial binds to the domain controller server, select one of the following options:

w/ Configured Credentials: Fill in the client distinguished name (**Client DN**) and **Password** to be used for the initial bind. If this bind

fails, the authentication process also fails. If the bind is successful, a search will attempt to find a user record that matches the client distinguished name entered in the **Client DN** field. The search typically looks for common attributes that might match the userid presented during the login process. These attributes include `displayName`, `sAMAccountName`, and `userPrincipalName`. If the **UID search attribute** field is configured, the search also includes this attribute.

If the search is successful, then a second bind is attempted, this time with the user distinguished name (retrieved from the search) and the password presented during the login process. If the second bind attempt succeeds, the authentication portion succeeds and group membership information for the user is retrieved and matched against the locally configured groups on the advanced management module. The matched groups will define the authorization permissions assigned to the user.

w/ Login Credentials: The initial bind to the domain controller server is made using the credentials presented during the login process. If this bind fails, the authentication process also fails. If the bind is successful, a search will attempt to find the user record. Once located, group membership information for the user is retrieved and matched against the locally configured groups on the advanced management module. The matched groups will define the authorization permissions assigned to the user.

9. To enable or disable SSL between the advanced management module and the Active Directory server, click **LDAP section of the security page**.

Active Directory role-based authentication and authorization:

You can set up remote LDAP authentication and authorization for users using Active Directory.

Note:

- Active Directory role-based authentication and authorization applies only to BladeCenter units deployed in an Active Directory environment.
- The Enhanced Role Based Security Snap-in tool is required for Active Directory role-based authentication and authorization.

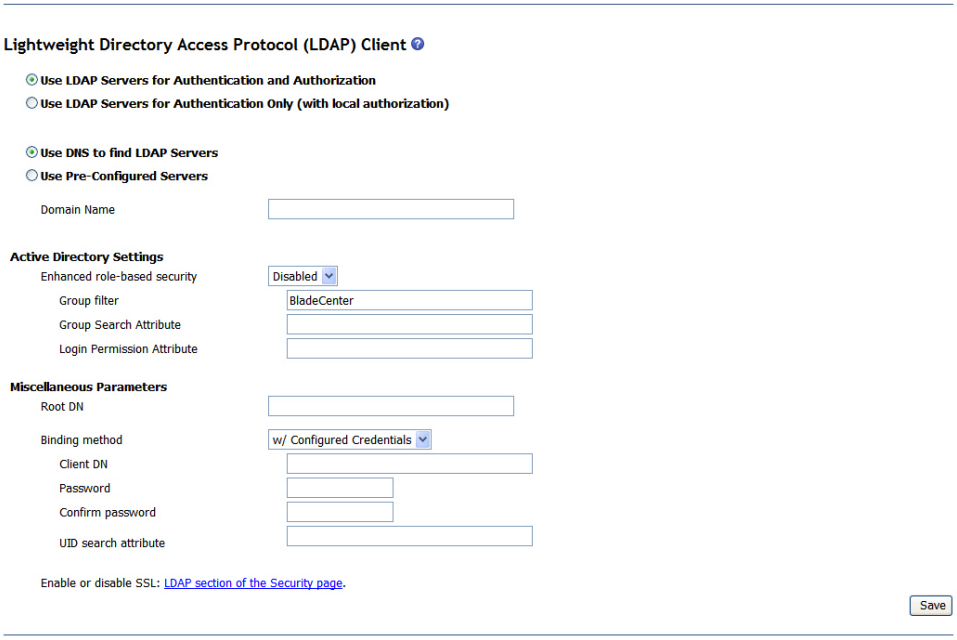
Active Directory role-based authentication and authorization uses configuration information stored on an Active Directory server to authenticate a user and then associate permissions with this user.

Before enabling Active Directory role-based authentication and authorization, use the Enhanced Role Based Security Snap-in tool to store the configuration information on the Active Directory server that associates permissions to users. This tool runs on any Microsoft Windows client and can be downloaded from http://www.ibm.com/systems/support/.

- The Enhanced Role Based Security Snap-in tool allows you to configure roles on an Active Directory server and to associate users, groups, and advanced management modules to these roles. See the documentation for the Enhanced Role Based Security Snap-in tool for information and instructions.
- Roles identify the permissions assigned to users and groups and identify the command targets, such as the advanced management module or a blade server, to which a role is attached. Before enabling Active Directory role-based authentication and authorization, roles should be configured on the Active Directory server.
- The optional name configured in the **AMM Target Name** field identifies a particular advanced management module and can be associated with one or more roles on the Active Directory server through the Role Based Security (RBS) Snap-In tool. This is accomplished by creating managed targets, giving them specific names, and associating them with the appropriate roles. If an **AMM Target Name** is configured, it can define specific roles for users and advanced management modules (targets) that are members of the same role. When a user logs in to the advanced management module and is authenticated through Active Directory, the roles for this user are retrieved from the directory. The permissions assigned to the user are extracted from the roles that also have a target as a member with a name that matches the advanced management module configured here, or a target that matches any advanced management module. Advanced management module can be given a unique name, or multiple advanced management modules can share the same target name. Assigning multiple advanced management modules to the same target name groups multiple advanced management modules together and assigns them to the same role.

To configure Active Directory role-based authentication and authorization for the advanced management module, complete 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.
3. Select **Use LDAP Servers for Authentication and Authorization**.
4. Set **Enhanced role-based security** to **Enabled**.
5. The domain controllers (DC) to be used for authentication can either be manually configured or discovered dynamically via DNS SVR records.
   - Select **Use DNS to find LDAP Servers** to dynamically discover the domain controllers based on DNS SVR records (see step 6).
   - Select **Use Pre-Configured LDAP Servers** (default) to manually configure the domain controllers (see step 7 on page 33).
6. If you are using DNS to dynamically discover the domain controllers, configure the domain name of the domain controller; then, go to step 8 on page 34.



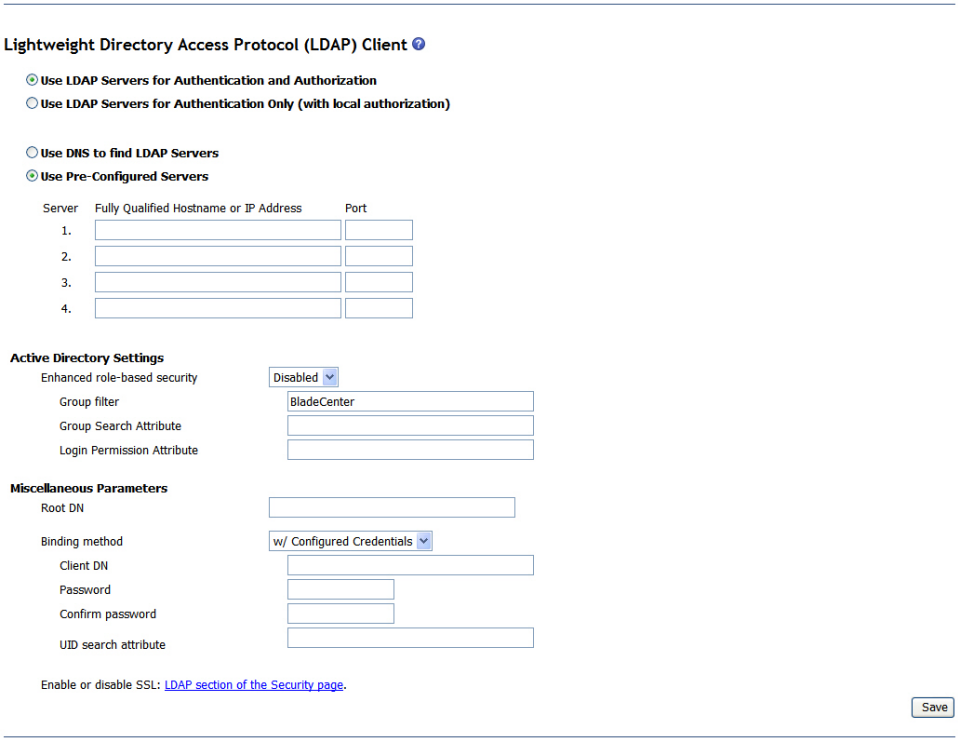
Domain Name

The fully qualified domain name of the domain controller. The domain name is needed to find the domain controller.

Active Directory Forest Name

Active Directory role-based authentication and authorization does not make use of Global Catalogs; leave this field blank.

7. If you are manually configuring the domain controllers, configure the **LDAP Server Host Name or IP Address** field; then, go to step 8 on page 34. Up to four domain controllers can be configured using an IP address or a fully qualified hostname.



8. Configure the following **Miscellaneous Parameters**:

Root DN

This optional parameter is used to configure the base distinguished name (DN) of the Active Directory server (for example, dn=companyABC,dn=com). In most cases, this field is left blank, although it can be useful for debugging purposes.

The advanced management module normally uses the RootDSE query to find the base distinguished name of an Active Directory server with which it communicates. This base distinguished name is then used for subsequent searches. The base distinguished name is derived from the `defaultNamingContext` and `rootDomaintNamingContext` attributes retrieved from the RootDSE query. When the base distinguished name is set using the **Root DN** field, it overrides the `defaultNamingContext` and `rootDomaintNamingContext` attributes.

Binding Method

For initial binds to the domain controller server, select one of the following options:

w/ Configured Credentials: Fill in the client distinguished name (**Client DN**) and **Password** to be used for the initial bind. If this bind fails, the authentication process also fails. If the bind is successful, a search will attempt to find a user record that matches the client distinguished name entered in the **Client DN** field. The search typically looks for common attributes that might match the userid presented during the login process. These attributes include `displayName`, `sAMAccountName`, and `userPrincipalName`. If the **UID search attribute** field is configured, the search also includes this attribute.

If the search is successful, then a second bind is attempted, this time with the user distinguished name (retrieved from the search) and the password presented during the login process. If the second bind

attempt succeeds, the authentication portion succeeds and group membership information for the user is retrieved and matched against the locally configured groups on the advanced management module. The matched groups will define the authorization permissions assigned to the user.

w/ Login Credentials: The initial bind to the domain controller server is made using the credentials presented during the login process. If this bind fails, the authentication process also fails. If the bind is successful, a search will attempt to find the user record. Once located, group membership information for the user is retrieved and matched against the locally configured groups on the advanced management module. The matched groups will define the authorization permissions assigned to the user.

9. To enable or disable SSL between the advanced management module and the Active Directory server, click **LDAP section of the security page**.

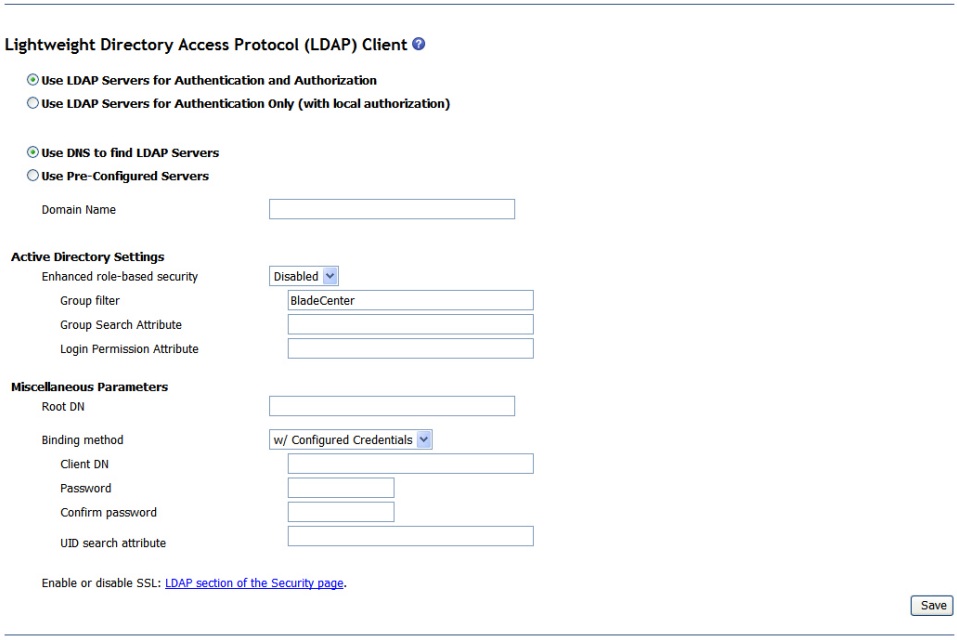
Legacy LDAP authentication and authorization:

You can configure LDAP search attributes for an advanced management module on which enhanced role-based security for Active Directory users is disabled.

Legacy LDAP authentication and authorization was the original model deployed on advanced management modules. It supports Active Directory, Novell eDirectory, and OpenLDAP environments and relies on configuration information stored on an LDAP server to associated permissions with a user. It is used to both authenticate and authorize users through an LDAP server.

Complete the following steps to configure legacy LDAP authentication and authorization:

1. In the navigation pane, click **MM Control → Network Protocols**.
2. Select **Use LDAP Servers for Authentication and Authorization**.
3. Set **Enhanced role-based security** to **Disabled**.
4. The LDAP servers to be used for authentication can either be manually configured or discovered dynamically via DNS SVR records.
   - Select **Use DNS to find LDAP Servers** to dynamically discover the LDAP servers based on DNS SVR records (see step 5).
   - Select **Use Pre-Configured LDAP Servers** (default) to manually configure the LDAP servers (see step 6 on page 36).
5. If you are using DNS to dynamically discover the LDAP servers, configure the domain name of the LDAP server; then, go to step 7 on page 37.



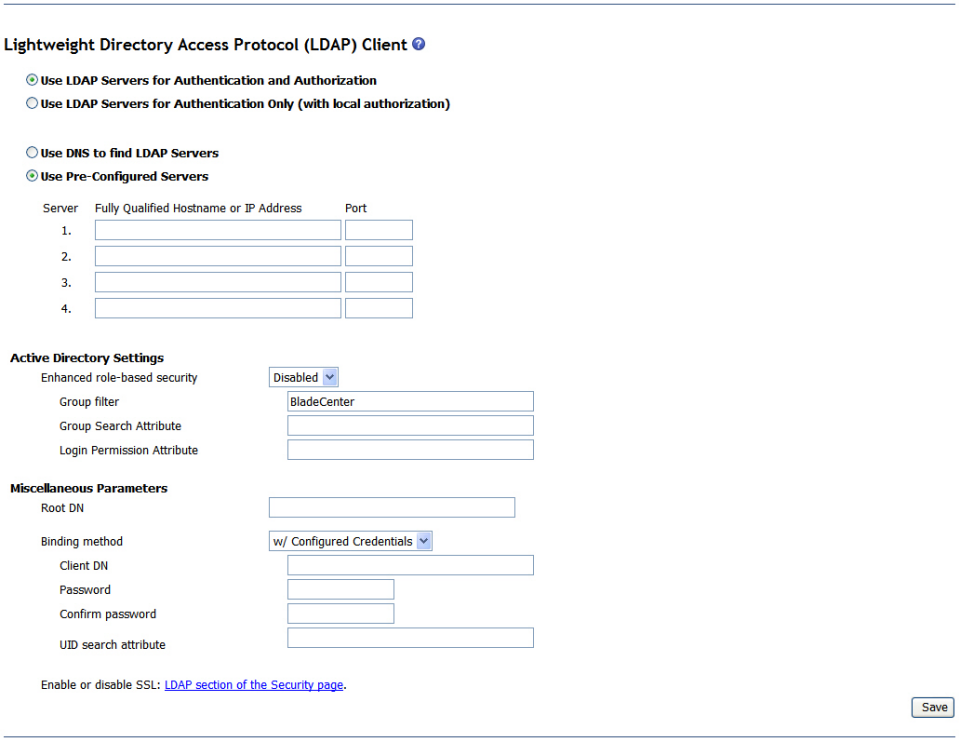
Domain Name

The fully qualified domain name of the LDAP server. The domain name is needed to find the LDAP server.

Active Directory Forest Name

Active Directory role-based authentication and authorization does not make use of Global Catalogs; leave this field blank.

6. If you are manually configuring the LDAP servers, configure the **LDAP Server Host Name or IP Address** field; then, go to step 7 on page 37. Up to four LDAP servers can be configured using an IP address or a fully qualified hostname.



7. Configure the following **Miscellaneous Parameters**:

Root DN

This optional parameter is used to configure the base distinguished name (DN) of the Active Directory server (for example, dn=companyABC,dn=com). In most cases, this field is left blank, although it can be useful for debugging purposes.

The advanced management module normally uses the RootDSE query to find the base distinguished name of an Active Directory server with which it communicates. This base distinguished name is then used for subsequent searches. The base distinguished name is derived from the `defaultNamingContext` and `rootDomaintNamingContext` attributes retrieved from the RootDSE query. When the base distinguished name is set using the **Root DN** field, it overrides the `defaultNamingContext` and `rootDomaintNamingContext` attributes.

Binding Method

For initial binds to the domain controller server, select one of the following options:

w/ Configured Credentials: Fill in the client distinguished name (**Client DN**) and **Password** to be used for the initial bind. If this bind fails, the authentication process also fails. If the bind is successful, a search will attempt to find a user record that matches the client distinguished name entered in the **Client DN** field. The search typically looks for common attributes that might match the userid presented during the login process. These attributes include `displayName`, `sAMAccountName`, and `userPrincipalName`. If the **UID search attribute** field is configured, the search also includes this attribute.

If the search is successful, then a second bind is attempted, this time with the user distinguished name (retrieved from the search) and the password presented during the login process. If the second bind attempt succeeds, the authentication portion succeeds and group membership information for the user is retrieved and matched against the locally configured groups on the advanced management module. The matched groups will define the authorization permissions assigned to the user.

w/ Login Credentials: The initial bind to the domain controller server is made using the credentials presented during the login process. If this bind fails, the authentication process also fails. If the bind is successful, a search will attempt to find the user record. Once located, group membership information for the user is retrieved and matched against the locally configured groups on the advanced management module. The matched groups will define the authorization permissions assigned to the user.

8. Configure the following **Active Directory Settings**:

Group Filter

The **Group Filter** field is used for group authentication. It specifies the groups that the advanced management module belongs to. If the **Group Filter** field left blank, group authentication is disabled. If enabled, group authentication 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, then group authentication passes. All comparisons that are made during authentication are case sensitive.

When group authentication is disabled, user records must contain the permission attribute, otherwise access will be denied (see Login Permission Attribute). For each group that matches the group filter, the permissions associated with that group are assigned to the user. The permissions associated with a group are found by retrieving the Login Permission Attribute from the group record.

The group filter is limited to 511 characters and can contain multiple group names. A colon (:) *must* be used to delimit group names. Leading spaces and trailing spaces are ignored; all other spaces are treated as part of the group name. An asterisk (*) wildcard character is not treated as a wildcard, the wildcard concept being removed for security reasons. 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 by using the actual domain name or by using adminGroup.

Group Search Attribute

This field is used by the search algorithm to find group membership information for a specific user. When the group filter name is configured, the list of groups to which the 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.

In an Active Directory or Novell eDirectory environment, the group search attribute specifies the attribute name that identifies the groups that a user belongs to. In Active Directory, this is usually `memberOf`, and with Novell eDirectory, this is usually `groupMembership`. In an OpenLDAP server environment, users are typically assigned to groups whose `objectClass` equals PosixGroup. In that context, this parameter specifies the attribute name that identifies the members of a particular PosixGroup; this is usually `memberUid`.

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.

This field must not be left blank; otherwise, it is impossible to retrieve the user permissions. Without verified permissions, the login attempt will fail. This is a different from some earlier releases, where access was granted with default read-only permissions assigned to the user whose permissions could not be verified.

The attribute value that is returned by the LDAP server is searched for the keyword string “IBMRBSPermissions=”. This keyword must be immediately followed by a bit string entered as 64 consecutive 0's or 1's. Each bit represents a particular set of functions. The bits are numbered according to their position; the leftmost bit is bit position 0. A value of 1 at a position enables the corresponding function. A value of 0 disables that function. The string “IBMRBSPermissions=010000000000” is a valid example.

Note that the “IBMRBSPermissions=” keyword is used to enable it to be placed anywhere in the attribute field. This enables the LDAP administrator to reuse an existing attribute, preventing an extension to the LDAP schema. Furthermore, this enables the attribute to be used for its original purpose. The keyword string can be added anywhere. The attribute that you use should enable a free-formatted string.

Note: To make the task of configuring users easier when you are using a Microsoft Windows platform, a Role Based Security (RBS) snap-in utility is available at http://www-304.ibm.com/jct01004c/systems/support/supportsite.wss/docdisplay?lndocid=MIGR-5069735&brandind=5000008. The snap-in utility configures roles on an Active

Directory server and associates users, groups, and advanced management modules to those roles.

The permission bits are interpreted as follows:

- Deny Always (bit position 0): If this bit is set, the user will always fail authentication. This function can be used to block a particular user or users associated with a particular group.
- Supervisor Access (bit position 1): If this bit is set, the user is given administrator privileges, which lets the user view any page, enables changes to any field, and permits all actions provided by the interface. When this bit is set, the other bits that define specific function access do not have to be set individually. This user is the only user who can back up the advanced management module configuration to the BladeCenter unit or to restore a backed up advanced management module configuration.
- Read Only Access (bit position 2): If this bit is set, the 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, the user can modify the settings in the **Security**, **Network Protocols**, and **Network Interface** pages for **MM Control**. If this bit is set, the user also can modify the IP configuration parameters for I/O modules under the **I/O Module Tasks → Management** page.
- User Account Management (bit position 4): If this bit is set, the 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, the user can access a remote blade server video console with keyboard and mouse control.
- Blade Server Remote Console and Virtual Media Access (bit position 6): If this bit is set, the user can access a remote blade server video console with keyboard and mouse control and also can access the virtual media features for that remote blade server.
- Blade Server and I/O Module Power/Restart Access (bit position 7): If this bit is set, the user can access the power-on and restart functions for the blade servers and the I/O modules. These functions are available in the **Blade Tasks → Power/Restart** page and the **I/O Module Tasks → Power/Restart** page.
- Basic Configuration (bit position 8): If this bit is set, the user can modify basic configuration parameters for the management module and blade servers. These parameters include the **General Settings** and **Alerts** pages of **MM Control** and the **Configuration** page of the **Blade Tasks**.
- Ability to Clear Event Logs (bit position 9): If this bit is set, the user can clear the event logs. All users can view the event logs, but this permission is required to clear the event logs.
- Advanced Adapter Configuration (bit position 10): If this bit is set, the user has no restrictions when configuring the management module, blade servers, I/O modules, and VPD. In addition, the user has administrative access, meaning that this user also can perform

the following advanced functions: firmware upgrades on management module or blade servers, restore management module factory defaults, modify and restore the management module configuration from a configuration file, and restart or reset the management module.

- Version Number (bit positions 11 through 15): A version number of 00000 indicates that the user permissions scheme that is set using bit positions 0 through 10 is used. A version number of 00001 indicates that the role-based user permissions scheme using bit positions 16 through 55 is used. Any other version number will use the user permissions scheme that is set using bit positions 0 through 10.
- Deny Always Role (bit position 16): If this bit is set, the user will always fail authentication. This function can be used to block a particular user or users associated with a particular group.
- Supervisor Role (bit position 17): If this bit is set, the user has no restrictions. The user has read/write access to all pages and fields for all devices. When this bit is set, there is no need to set any other authority levels that are controlled by bits 18 through 55.
- Operator Role (bit position 18): If this bit is set, the user has read-only access. This user cannot perform any maintenance procedures (for example, restart, remote actions, firmware updates) and is unable to modify any settings (using the save, clear, or restore functions). Note that read-only and all other bits are mutually exclusive, with read-only having the lowest precedence. That is, if any other bit is set, this bit 18 is ignored.
- Chassis Operator Role (bit position 19): If this bit is set, the user can browse status and properties of BladeCenter unit components (management module, blowers, midplane, power modules, media tray) and can back up the management module configuration. This user also can back up the advanced management module configuration to a file.
- Chassis User Account Management Role (bit position 20): If this bit is set, the user can add, modify, and delete users in the **MM Control → Login Profiles** page. Changing the global login settings requires the Chassis Configuration role. This user also can back up the advanced management module configuration to a file.
- Chassis Log Account Management Role (bit position 21): If this bit is set, the user can clear the event logs or change the log policy settings. All users can view the event logs, but this role is required to clear the logs or to change the log policy settings (the field at the top of the event log page). This user also can back up the advanced management module configuration to a file.
- Chassis Configuration Role (bit position 22): If this bit is set, the user can modify and save any BladeCenter unit configuration parameter except user profiles and event log settings; (for example, general management module settings, management module port assignments, management module network interfaces, management module network protocols, and management module security). This user also can change the SOL configuration under the SOL configuration web page, the ability to change the global login settings, and the ability to back up the advanced management module configuration to a file. In addition, this user can restore management module factory defaults configuration, if the user also has Chassis Administration permissions.

- Chassis Administration Role (bit position 23): If this bit is set, the user can perform management module firmware updates, modify the state of the BladeCenter unit LEDs, and restart the management module. The user also can restore management-module factory defaults configuration if the user also has Chassis Configuration permissions.
- Blade Operator Role (bit position 24): If this bit is set, the user can read blade information but not to modify it.
- Blade Remote Presence Role (bit position 25): If this bit is set, the user can access the Remote Control web page and the functions that are provided on the page: remote console (KVM) and remote disk. In addition, this user can issue the command-line interface (CLI) console command to start an SOL session to a blade server.
- Blade Configuration Role (bit position 26): If this bit is set, the user can modify and save any blade server configuration parameter except parameters in the SOL configuration web page (for example, blade server names, blade server policy settings, and can disable or enable SOL for individual blade servers on the Serial Over LAN status web page).
- Blade Administration Role (bit position 27): If this bit is set, the user can power-on, power-off, and restart blade servers, activate standby blade servers, do firmware updates, and modify the state of blade server LEDs.
- Switch Operator Role (bit position 28): If this bit is set, the user can browse the status and properties of I/O modules and the ability to ping I/O modules.
- Switch Configuration Role (bit position 29): If this bit is set, the user can configure the I/O module IP address, enable or disable external management over all ports, and preserve new IP configuration on all resets. The user also can restore factory defaults and to start a Telnet or web session to an I/O module, if the user also has Switch Administration permissions.
- Switch Administration Role (bit position 30): If this bit is set, the user can power-on, power-off, and restart I/O modules with various diagnostic levels, update passthru I/O module firmware, enable or disable Fast POST, and enable or disable external ports. The user also can restore factory defaults and to start a Telnet or web session to an I/O module, if the user also has Switch Configuration permissions.
- Blade 1 Scope (bit position 31): If this bit is set, the user has access to the blade server in bay 1.
- Blade 2 Scope (bit position 32): If this bit is set, the user has access to the blade server in bay 2.
- Blade 3 Scope (bit position 33): If this bit is set, the user has access to the blade server in bay 3.
- Blade 4 Scope (bit position 34): If this bit is set, the user has access to the blade server in bay 4.
- Blade 5 Scope (bit position 35): If this bit is set, the user has access to the blade server in bay 5.
- Blade 6 Scope (bit position 36): If this bit is set, the user has access to the blade server in bay 6.
- Blade 7 Scope (bit position 37): If this bit is set, the user has access to the blade server in bay 7.

- Blade 8 Scope (bit position 38): If this bit is set, the user has access to the blade server in bay 8.
- Blade 9 Scope (bit position 39): If this bit is set, the user has access to the blade server in bay 9.
- Blade 10 Scope (bit position 40): If this bit is set, the user has access to the blade server in bay 10.
- Blade 11 Scope (bit position 41): If this bit is set, the user has access to the blade server in bay 11.
- Blade 12 Scope (bit position 42): If this bit is set, the user has access to the blade server in bay 12.
- Blade 13 Scope (bit position 43): If this bit is set, the user has access to the blade server in bay 13.
- Blade 14 Scope (bit position 44): If this bit is set, the user has access to the blade server in bay 14.
- Chassis Scope (bit position 45): If this bit is set, the user has access to the BladeCenter unit and management module.
- I/O Module 1 Scope (bit position 46): If this bit is set, the user has access to I/O module 1.
- I/O Module 2 Scope (bit position 47): If this bit is set, the user has access to I/O module 2.
- I/O Module 3 Scope (bit position 48): If this bit is set, the user has access to I/O module 3.
- I/O Module 4 Scope (bit position 49): If this bit is set, the user has access to I/O module 4.
- I/O Module 5 Scope (bit position 50): If this bit is set, the user has access to I/O module 5.
- I/O Module 6 Scope (bit position 51): If this bit is set, the user has access to I/O module 6.
- I/O Module 7 Scope (bit position 52): If this bit is set, the user has access to I/O module 7.
- I/O Module 8 Scope (bit position 53): If this bit is set, the user has access to I/O module 8.
- I/O Module 9 Scope (bit position 54): If this bit is set, the user has access to I/O module 9.
- I/O Module 10 Scope (bit position 55): If this bit is set, the user has access to I/O module 10.
- Reserved (bit position 56 through 63): reserved for future use.

If none of the bits are set, the default is set to deny always (read-only) for the user.

Note that priority is given to login permissions that are retrieved directly from the user record. If the user does not have the login permission attribute in the user record, an attempt is made to retrieve the permissions from the groups that the user belongs to. 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. Again, the Deny Always bit is set only if all the other bits are zero. Also note that 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.

Important: If you give a user the ability to modify basic, networking, or security related adapter configuration parameters, consider giving this same user the ability to restart the management module. If the user is unable to reset the management module, changes that the user makes that require a restart will not take effect.

9. To enable or disable SSL between the advanced management module and the Active Directory server, click **LDAP section of the security page**.

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 SSL settings from the **MM Control → Security** page; you can enable or disable SSL and manage the certificates that are required for SSL. Changes made to the SSL server settings are effective immediately for the advanced management module; you do not need to restart the advanced management module.

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 46.

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 46.)
   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 53.)
2. Configure the SSL client certificates for secure LDAP connections:

   Note: SSL client certificate management is optional. You can still enable the SSL client for LDAP without generating a self-signed certificate or importing a signed certificate to the client.
   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 53.)
   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 54.)
   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 55.)

   Notes:
   - Changes to the SSL client configuration take effect immediately and do not require a restart of the management module.
   - For the advanced management module, the following configuration changes to the SSH, SMASH, and Secure SMASH no longer require a restart of the advanced management module:
     - Enable/disable SSH or Secure SMASH
     - Generate new SSH Host Keys
     - Change the port number for SSH or Secure SMASH
     - Install, delete or modify SSH public keys that are used for authentication

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:

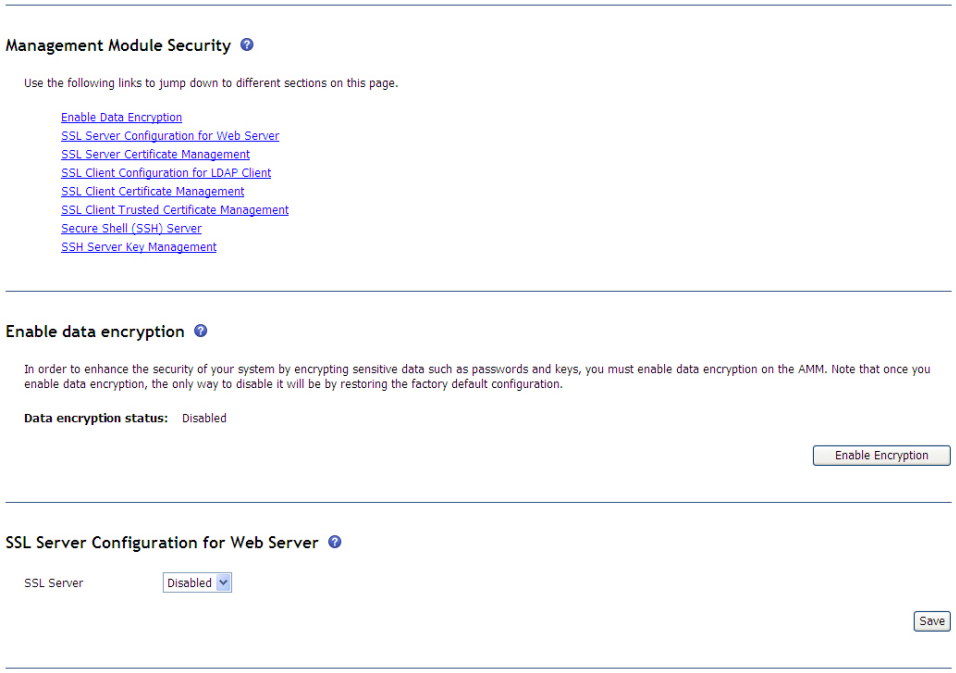
The SSL server requires that a valid certificate and corresponding private encryption key be installed before SSL is enabled.

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” on page 47. To use a certificate-authority-signed certificate for the SSL server, see “Generating a certificate signing request” on page 48.

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.



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

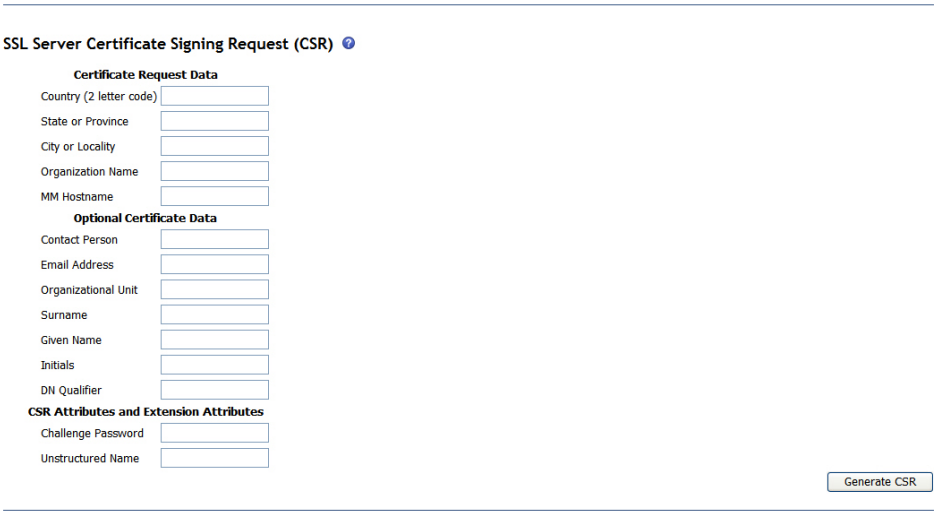
4. Type the information in the required fields and any optional fields that apply to your configuration. For a description of the fields, see Required certificate data. After you finish typing the information, click **Generate Certificate**. Your new

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.

Generating a certificate signing request:

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

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



4. Type the information in the required fields and any optional fields that apply to your configuration. The fields are the same as 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.

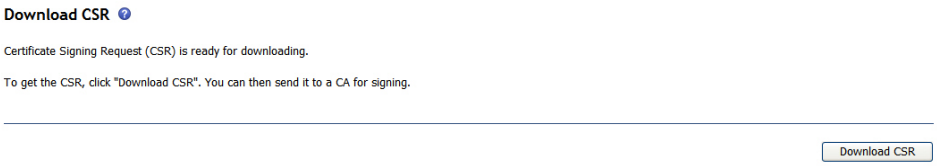
- **Certificate-signing request attributes**

  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.



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
   ```

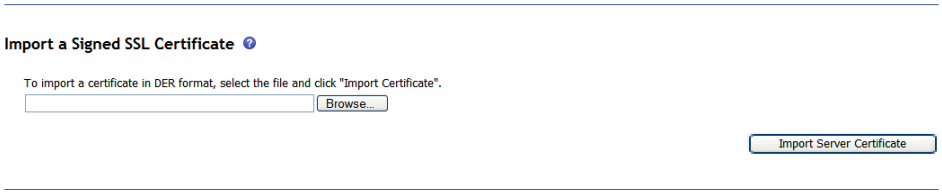
7. Send the certificate signing request to your certificate authority. When the certificate authority returns your signed certificate, you might need to convert the certificate to DER format. (If you received the certificate as text in an email or a web page, it is probably in PEM format.) You can change 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 52 after the signed certificate is returned from the certificate authority.

8. In the navigation pane, click **MM Control → Security**. Scroll to the **SSL Server Certificate Management** section, which looks similar to the page in the following illustration.

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



10. Click **Browse**.
11. Click the certificate file that you want; then, click **Open**. The file name (including the full path) is displayed in the field next to the **Browse** push button.
12. Click **Import Server Certificate** to begin the process. A progress indicator is displayed as the file is transferred to storage on the management module. 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 46.

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.

Note: SSL client certificate management is optional. You can still enable the SSL client for LDAP without generating a self-signed certificate or importing a signed certificate to the client.

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 47. To use a certificate-authority-signed certificate for the SSL client, see "Generating a certificate signing request" on page 48.

SSL client trusted certificate management:

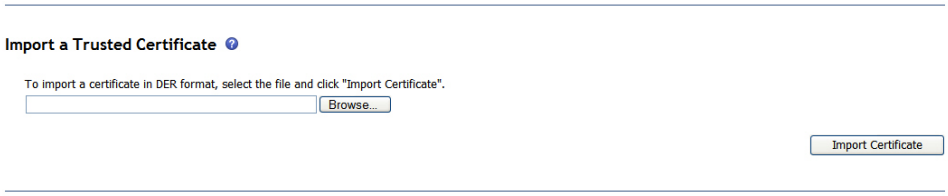
The secure SSL client (LDAP client) uses trusted certificates to positively identify the LDAP server.

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 Certificate** 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 Certificate 1 option. To remove a trusted certificate, click the corresponding **Remove** button.

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

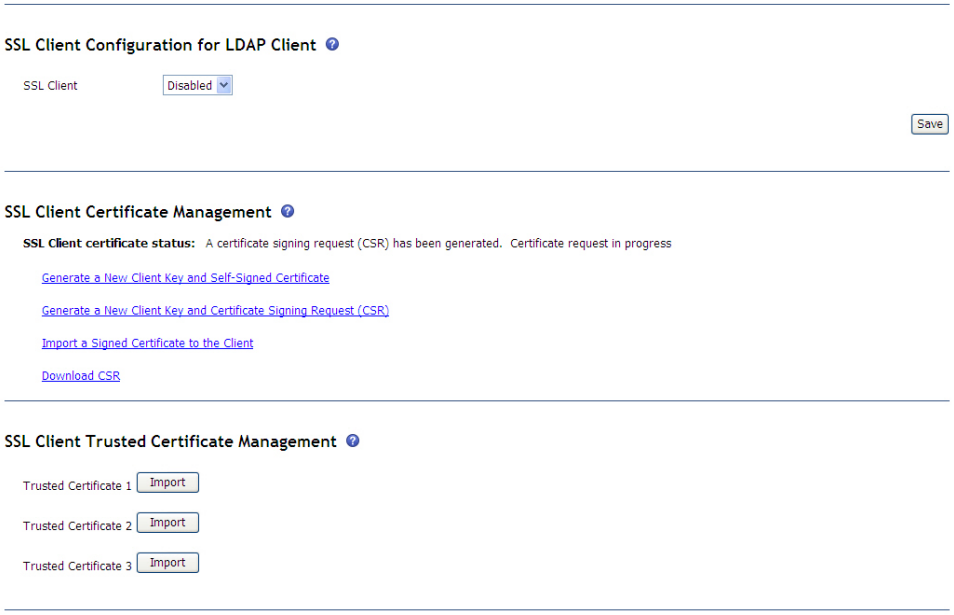
Enabling SSL for the LDAP client:

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** and scroll to the **SSL Client Configuration for LDAP Client** section. A page similar to the one in the following illustration is displayed.



   The **MM Control → Security** page shows an installed SSL client certificate and Trusted CA Certificate 1.
2. On the **SSL Client Configuration for LDAP Client** page, select **Enabled** in the **SSL Client** field.
3. Click **Save**. The 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 public key authentication or password authentication. Public key authentication is supported on only the advanced management module. SSH is enabled on the advanced management module by default, and a host key is automatically generated for SSH.

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:

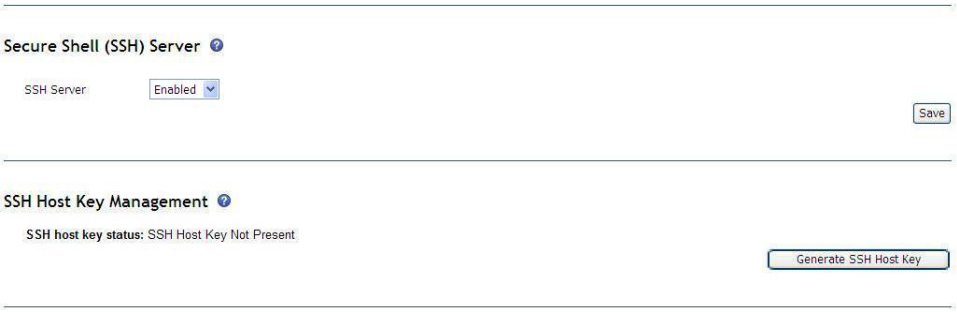
You can generate a Secure Shell host key to authenticate the identity of the Secure Shell server to the client.

For the advanced management module, the host keys are generated automatically if no host keys exist when the SSH server is enabled or when Secure SMASH is enabled. The Secure Shell server cannot be used until key generation is complete, which can take from 3 to 5 minutes. The event log records when the key generation starts and when it is completed.

When you request a new host key, both an RSA key and a DSA key are created to enable 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 **SSH Server/Host Key Management** section. A page similar to the one in the following illustration is displayed.



3. Click **Generate SSH Host Key**.

The key generation process is started in the background. You can check the progress of key generation by consulting the event log. If the SSH server is enabled, it is automatically restarted with the new host key after the key is generated.

Enabling the Secure Shell server:

SSH is enabled on the advanced management module by default, and a host key is automatically generated for SSH.

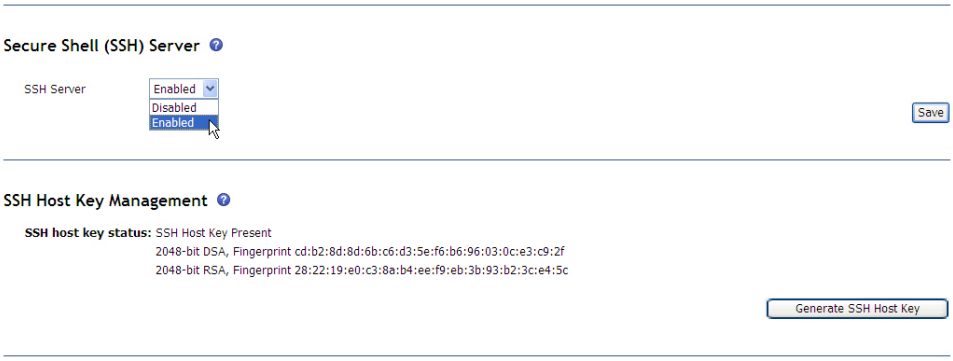
The value that is displayed on the page (Enabled or Disabled) is the last selected value and is the value that is used when the management module is restarted. For the advanced management module, these changes take effect immediately.

Notes:

- You can enable the Secure Shell server only if a valid Secure Shell host key is installed.
- For the advanced management module, the SSH and Secure SMASH interfaces are enabled by default.
- For the advanced management module, the Secure Shell server also can be enabled or disabled through SNMP or the management-module command-line interface. See the *BladeCenter Advanced Management Module Command-Line Interface Reference Guide* for more information.

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.



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

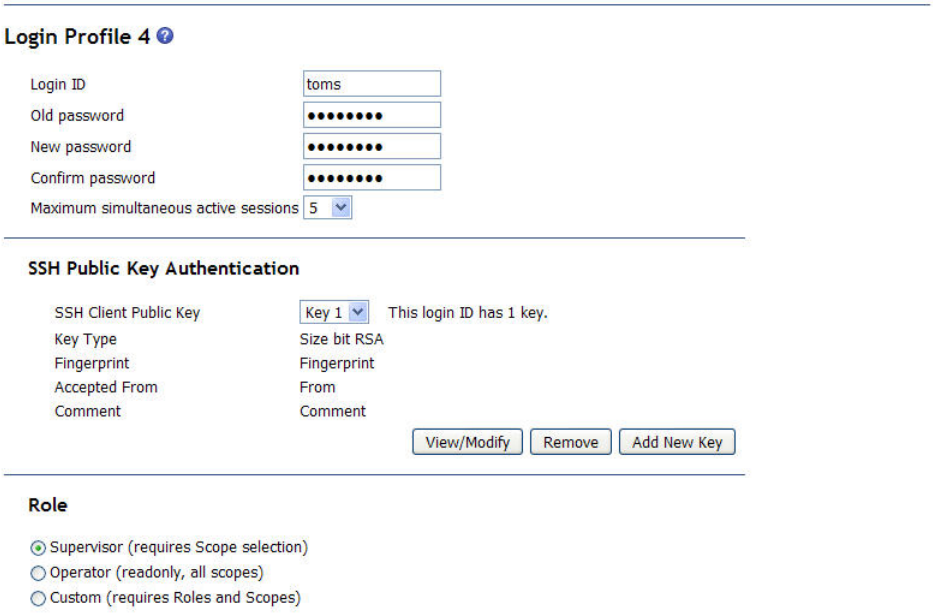
Assigning an SSH public key:

You can use SSH Public Key Authentication to access SSH or Secure SMASH without using a password.

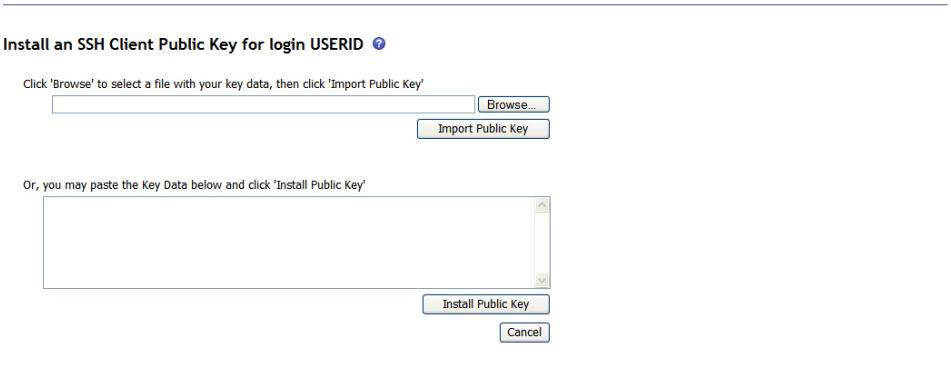
You can import up to four SSH private keys per Login Profile, subject to the advanced management module system limit of 12 keys.

Public keys are assigned to specified users. To assign a public key, complete the following steps:

1. In the navigation pane, click **MM Control → Login profiles**. If the Login ID is not displayed, you must enter a login ID and password, confirm the password, and save this information. Then proceed to step 2.
2. Select the login ID that you want to use. A page similar to the one in the following illustration is displayed.



3. To assign a new public key to the selected user, click **Add New Key**. A page similar to the one in the following illustration is displayed.



4. If the public key can be accessed through your directory system, click **Browse** to locate the file that you want to use; then, click **Import Public Key.**
5. If the public key data is in an open document, copy the data and paste it into the designated field; then, click **Install Public Key**

For further information about viewing, modifying, and deleting public keys, see "Login Profiles" on page 151.

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.

The advanced management module supports non-interactive Secure Shell sessions. This support is most useful when it is combined with public key authentication. Use this capability to issue a single CLI command by adding the command to the end of the ssh command. For example, to get a list of the current users of the advanced management module, type

```
ssh -l USERID 192.168.70.2 users -T mm[1] -curr
```

If the CLI command requires a special character such as a quotation mark, precede the character with an escape sequence so that it is processed correctly by the command shell on your client system. For example, to set a new trespass warning, type a command similar to the following command:

```
ssh -l USERID 192.168.70.2 trespass -T mm[1] -tw \"New  WARNING\"
```

To start a Serial over LAN text redirection session to a blade server the process is similar, but in this case it is important to specify that the Secure Shell server session uses a pseudo-terminal (PTY) to get the correct output formatting and keystroke handling. In the following example, which starts a Serial over LAN session to the blade server in bay 2, the ssh client option `-t` specifies that a pseudo-terminal should be allocated:

```
ssh -t -l USERID 192.168.70.1 console -T blade[2]
```

Enabling SMASH

You can set the advanced management module to use the System Management Architecture for Server Hardware Command Line Protocol (SMASH CLP).

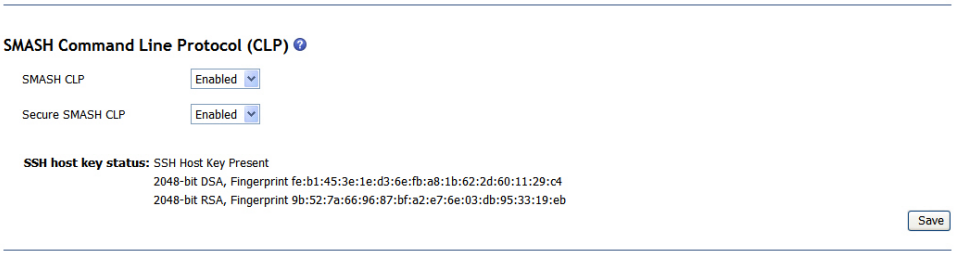
From the Network Protocols page, you can enable or disable the SMASH or Secure SMASH command line protocols. These changes take effect immediately.

Notes:

- To use the SMASH interface, you must use a login ID that is defined on the Login Profiles page. LDAP-authenticated users cannot access the SMASH interfaces.
- The Secure SMASH interface is enabled by default.
- If no SSH host key is present when the secure SMASH CLP is enabled, the SSH host key is generated automatically. SSH host key generation can take up to 5 minutes. Key generation completion is recorded in the event log.
- See the *IBM SMASH Proxy Installation and User's Guide* for more information.

To enable the SMASH command line protocol, complete the following steps:

1. In the navigation pane, click **Network Protocols**.
2. Scroll to the **SMASH Command Line Protocol (CLP)** section. A page similar to the one in the following illustration is displayed.



3. To enable the SMASH command line protocol over Telnet, click **Enabled** in the **SMASH CLP** field. The selected value (Enabled/Disabled) takes effect immediately.
4. To enable the Secure SMASH command line protocol over SSH, click **Enabled** in the **Secure SMASH CLP** field. The selected value (Enabled/Disabled) takes effect immediately.
5. Click **Save**.

Using SMASH:

You can use the System Management Architecture for Server Hardware Command Line Protocol (SMASH CLP) to communicate with the advanced management module. See the *IBM SMASH Proxy Installation and User's Guide* for more information.

To start an interactive SMASH CLP session by using an SSH client such as OpenSSH client with an advanced management module with networking address 192.168.70.2, type a command similar to the following example:

```
ssh -p 50022 -l USERID 192.168.70.2
```

where `-p 50022` specifies TCP port 50022, the default port number for Secure SMASH on the advanced management module and `-l USERID` specifies one of the 12 local account login IDs.

The advanced management module supports non-interactive Secure SMASH sessions. This support is most useful when it is combined with public key authentication. Use this capability to issue a single SMASH CLP command. To start a non-interactive SMASH session it is important to specify that the Secure SMASH server uses a pseudo-terminal (PTY). If you fail to specify a pseudo-terminal for the session, the error message `Input Redirection not Supported` is displayed. For example, to get a list of the SMASH-addressable entities, type a command similar to the following command:

```
ssh -t -p 50022 -l USERID 192.168.70.2 show /modular1
```

where `-t` specifies that a pseudo-terminal is required for the session and `show /modular1` is the SMASH command that is to be executed on the advanced management module.

If you are using a Telnet client to start an interactive SMASH CLP session you must specify the correct TCP port number. By default, the port that is assigned to the SMASH protocol is 50023.

Enabling Syslog

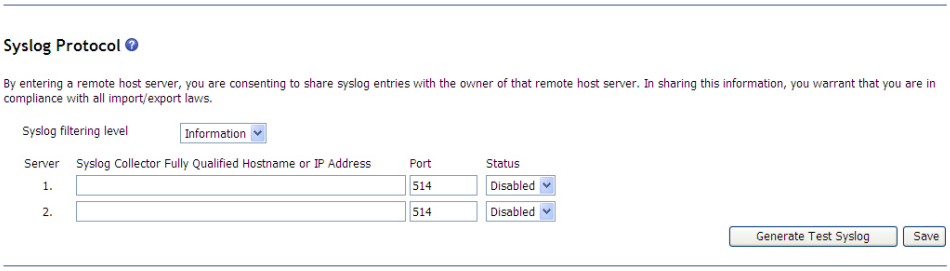
Select **MM Control → Network Protocols** to enable or disable the syslog protocol.

The syslog protocol provides a method for the advanced management module to send event log messages in a standard format through the network to up to two syslog collectors in compliance with RFC 3164. This method is useful because the advanced management module event log has a limited capacity and when it is full, it wraps, and the oldest entries are overwritten. By configuring syslog collectors, you will prevent the loss of any event history. The advanced management module syslog service is disabled by default. You can enable it and configure the syslog collectors by specifying their IP addresses, host names, and port numbers (the default port number is 514). The advanced management module also provides the ability to filter the transmitted log messages by minimum severity level for all targets.

Note: For the advanced management module, these changes take effect immediately.

To enable the syslog protocol, complete the following steps:

1. In the navigation pane, click **Network Protocols**.
2. Scroll to the **Syslog Protocol** section. A page similar to the one in the following illustration is displayed.



3. Use the **Syslog filtering level** field to specify which event log entries are forwarded to the remote syslog collector according to the event severity level.
   - **Error**: Forward event log entries with severity level Error to the remote syslog collector.
   - **Warning**: Forward event log entries with severity level Error or Warning to the remote syslog collector.
   - **Information**: Forward all event log entries to the remote syslog collector.
4. Use the **Syslog Collector Host Name or IP Address** fields to specify either the IP address or, if DNS is enabled and configured, the host name of the syslog collector. Up to two syslog collectors can be specified.
5. Use the **Port** field to specify the destination port number to receive advanced management module event logs on the syslog collector.
6. Select **Enabled** or **Disabled** in the **Status** field to specify whether you want to send management module event logs to the syslog collector.

Click **Generate Test Syslog** to generate a test syslog packet that verifies that the syslog collector information is correctly configured.

Configuring Linux TFTP server

You need to modify the configuration of Linux-based TFTP servers to support some automated features, such as service advisor.

In order to automatically put a service data file to a specified server using TFTP when a call home event is detected, the configuration file tftp must be modified to include the option that enables the creation of files on the TFTP server. Complete the following steps:

1. Open the TFTP configuration file in the /etc/xinet.d directory.
2. Add the -c option to the server_args argument.
3. Save and close the file.
4. Restart the TFTP server, using the `/etc/rc.d/init.d/xinetd restart` command.

The following example shows a configuration file /etc/xinetd.d/tftp with -c option added to the server argument:

Modified /etc/xinetd.d/tftp contents

```
service tftp
{
socket_type             = dgram
protocol                = udp
wait                    = yes
user                    = root
server                  = /usr/sbin/in.tftpd
server_args             = -c -s /tftpboot
disable                 = no
per_source              = 11
cps                     = 100 2
flags                   = IPv4
}
```

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 67

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. The advanced management module also enables you to save the management-module configuration to the backplane of the BladeCenter unit. Backup of the management module configuration requires special user permissions (see "Web interface pages and user roles" on page 88 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 an advanced management module configuration:

You can back up the configuration for an advanced 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 11.
2. In the navigation pane, click **MM Control → Configuration Mgmt**.
3. Select the type of backup that you want to perform:
   - **Backup Configuration to File**
   - **Save Configuration to Chassis**

   Notes:
   - If data encryption is enabled for the BladeCenter unit, you must enter a password for the configuration file. This password must be entered when you restore the configuration file.
   - Configuration files that are saved from BladeCenter units where data encryption is enabled can be used only with advanced management module firmware versions that support data encryption.
   - If data encryption is enabled for the BladeCenter unit and the BladeCenter unit Universally Unique Identifier (UUID) is modified, configuration data that is backed up to the BladeCenter unit becomes invalid: you must back up the configuration again after you change the UUID.

   a. To save the configuration to the BladeCenter unit, click **Save**. When you back up the configuration for BladeCenter units other than BladeCenter H units, click **Save (compressed format)** to save the configuration in a compressed format that requires less space. (BladeCenter H units automatically save the configuration in compressed format.)

   b. To back up the configuration to a file, click **View the current configuration summary** in the **Backup Configuration to File** section and complete the following steps.

      Note: The security settings for data encryption on the Security page are not backed up.

      1) Verify the settings; then, click **Close**.
      2) To back up the configuration, click **Backup**.
      3) 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, click **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. The advanced management module also enables you to restore a configuration that was previously saved to the backplane of the BladeCenter unit. Restoring the management module configuration requires special user permissions (see "Web interface pages and user roles" on page 88 for 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 11.
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 can be changed 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 44.

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.

Restoring an advanced management-module configuration:

You can restore a saved configuration for an advanced management module.

To restore or modify your current configuration, complete the following steps. You can restore an advanced management module configuration only if it was previously saved to the BladeCenter unit or external media, as described in "Backing up an advanced management module configuration" on page 66.

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 11.
2. In the navigation pane, click **MM Control → Configuration Mgmt**.
3. Select the type of restoration that you want to perform: **Restore Defaults**, **Restore Configuration from File**, or **Restore Configuration from Chassis**.
   a. To restore the default configuration, click one of the following options:
      - **Restore Defaults:** Restore the management module to factory settings
      - **Restore Defaults Preserve Logs:** Restore the management module to factory settings while retaining the content of the management-module event log.

      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.
   b. If you are restoring the configuration from a file, click **Browse** in the **Restore Configuration from File** section and complete the following steps.

      Note: If the configuration file was saved from a BladeCenter unit where data encryption was enabled, you must enter the same password that was used to save the file.

      1) Click the configuration file that you want; then, click **Open**. The file (including the full path) is displayed in the field next to **Browse**.
      2) 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 can be changed are displayed. To change between this view and the complete configuration summary view, click **Toggle View** at the top or bottom of the window.
      3) To restore this file to the management module, click **Restore Configuration**. A progress indicator displays as the management module updates. 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 44.

A progress indicator displays as the firmware on the management module is updated. A confirmation window opens to indicate whether the update was successful.

c. To restore the configuration from the BladeCenter unit, click **Restore**; then, click **OK**. A progress indicator displays as the management module updates. A confirmation window opens to indicate whether the update was successful.

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

Using the remote console feature

The management module supports remote control of blade servers, as if you were at the local console.

The remote console allows you to access the video console of a blade server remotely, with keyboard and mouse control, using a stand-alone Java application window that launches when you click **Start Remote Control** from the **Blade Tasks → Remote Control** page. This separate browser window provides both the remote console and remote disk features (see "Using the remote disk feature" on page 70).

During a remote console session, only one blade server at a time can own the BladeCenter unit shared keyboard, video, and mouse (KVM). The remote console allows you to dynamically select which blade server controls the BladeCenter unit shared media tray, remote disk, and KVM (choices vary based on your BladeCenter unit type). Remote console sessions are terminated by closing the remote console window.

The remote console is a Java 2 applet that requires the Java Runtime Environment (JRE) plug-in. If the JRE plug-in is not installed and you are connected to the Internet, you will be prompted to install it; otherwise, you must obtain and install the JRE plug-in before you can use the remote console.

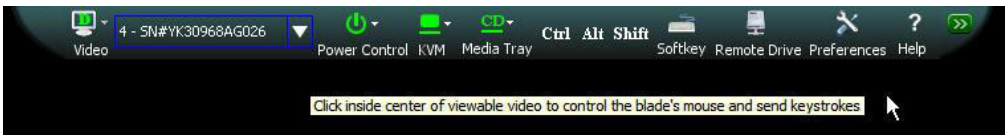
The remote console is supported by JRE version 6.0, update 10 or later.

Remote console supports the following standard VESA video modes:

- 640 x 480 - 60Hz, 72Hz, 75Hz, 85Hz
- 800 x 600 - 60Hz, 72Hz, 75Hz, 85Hz
- 1024 x 768 - 60Hz, 70Hz, 75Hz

All standard DOS VGA modes are supported.

The operating system of the remote console system you are using will trap certain key sequences, such as Ctrl+Alt+Del in Microsoft Windows, instead of transmitting them to the blade server. You can transmit these trapped key sequences by using the button bar that is at the top of the remote console window.



Using the remote disk feature

The management module can use remote mass storage devices.

From the Remote Control window (see "Remote Control" on page 123), you can assign, or mount, an optical drive, diskette drive, or USB drive that is on the remote client computer to a blade server. By using this window, you also can specify a disk image or CD (ISO) image on the remote system for the blade server to use or upload files to local storage on an advanced management module.

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 are the minimum server operating systems levels that support USB:

- Microsoft Windows Server 2003
- Microsoft Windows 2000 with Service Pack 4
- 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 6.0, update 10 or later installed. The client system must also have an Intel Pentium III or later microprocessor operating at 700 MHz or faster (or an equivalent microprocessor). A maximum of 15 remote disks can be mounted using Remote Control. This includes USB devices connected to the advanced management module and any disks mounted by other users.

Mounting a disk drive or image

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

To mount a disk drive or 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 11).
2. In the navigation pane, click **Blade Tasks → Remote Control**.
3. In the **Start Remote Control** section, click **Start Remote Control**.

   Note: USB key images have a file suffix of `.uki`. To create an image file of a USB flash key drive, use a binary copy tool and make sure that the image file has a file suffix of `.uki`.
4. Select the blade server that will have control of the media tray in the **Remote Disk** section.
5. In the **Remote Disk** section, select the resources to make available for mounting from the left side of the remote disk drive selector (labeled **Available Resources**); then, click **>>** to finalize the selection and move them to the right side of the remote disk drive selector (labeled **Selected Resources**). To deselect items, select them in the right side of the remote disk drive selector; then, click **<<**.

   You can upload a small disk image directly to the advanced management module flash memory (persistent) storage by selecting **Upload image to AMM** from the list of **Available Resources**. Advanced management module storage is used by other management-module features, so the amount of space that is available can vary.

   Saving the image to management module memory enables the image to remain mounted on the blade server so that you can access the image later, even if the web interface session is terminated. Mounted drives that are not saved to the management module are unmounted when the remote-control window is closed.
6. Click **Write Protect** to prevent data from being written to the mounted drives.
7. Select from the remote disk drive selector (labeled **Selected Resources**) one or more drives or images to mount; then, click **Mount Drive**. For an advanced management module that uses the concurrent-KVM feature, you can choose legacy operation (Chassis Media Tray Owner) or one of the cKVM blade servers from the **Mount remote media to** list. 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**.

Using management channel auto-discovery

You can use management channel auto-discovery (MCAD) to route BladeCenter management channel communications for MCAD-capable blade servers.

Note: The default state of the management channel auto-discovery feature is disabled. See "Enabling management channel auto-discovery" on page 73 for information about enabling this feature.

Management channel auto-discovery (MCAD) allows a blade server to select a communications channel used for management traffic within the BladeCenter unit and find an alternate channel if the current channel becomes unavailable. The blade server can select the default network interface card (NIC) on its system board, another NIC on the system board, or a port on an expansion card as the path for management traffic. Management channel auto-discover operations on the blade server are controlled by the blade system management processor (BSMP) or an MCAD-capable service processor. Management traffic routed by MCAD includes the following communications:

- SOL (Serial Over LAN)
- cKVM (concurrent KVM)
- FTP/TFTP
- Telnet
- BSMP service data and image flashing
- Chassis Internal Network (CIN)
- Other IP communication between the advanced management module and the blade server that take place over the BladeCenter internal management network

During MCAD operation, the blade server determines when it is appropriate to select the next best communication channel for management traffic and passes this information to the advanced management module.

The advanced management module calculates a list of communication channel candidates based on the list of channels available on the blade server as reported by the BSMP or service processor (this list is dependant on the hardware that is installed in the blade server) and the I/O modules that are installed in the BladeCenter unit. The advanced management module groups and prioritizes all ports in the candidate list, based on communication speed, and passes the list back to the blade server.

The blade server determines when to select the next best channel and which channel to select based on current management traffic conditions. The advanced management module responds to management packets it receives from the blade server, directing management traffic to the new network path.

The advanced management module reports which I/O module is currently being used for management traffic by each blade server and the status of the management traffic path. In BladeCenter units containing blade servers that do not support MCAD, these blades are automatically identified and route their management traffic using the standard non-MCAD method.

Enabling management channel auto-discovery

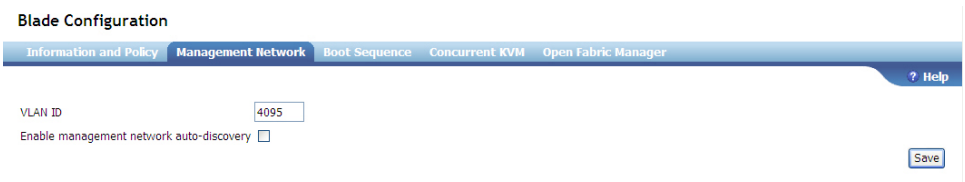
This topic discusses how to enable and disable management channel auto-discovery (MCAD) for the BladeCenter unit.

From the Blade Configuration page (see "Configuration" on page 129), you can enable or disable MCAD. The default setting for the MCAD feature is disabled.

Note: MCAD enablement is only available for MCAD-capable blade servers.

To enable or disable MCAD, complete the following steps:

1. In the navigation pane, click **Blade Tasks → Configuration**.
2. Select the to the **Management Network** tab. A page similar to the one in the following illustration is displayed.

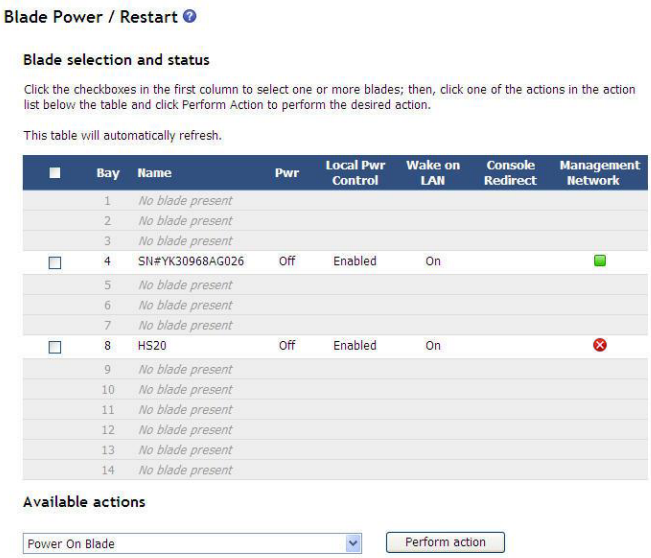


3. Select **Enabled** or **Disabled** in the **Enable management network auto-discovery** field to specify whether you want the management communications channel to be controlled by the blade server iBMC.

Viewing management channel auto-discovery status

You can view the management channel auto-discovery (MCAD) status for each blade server.

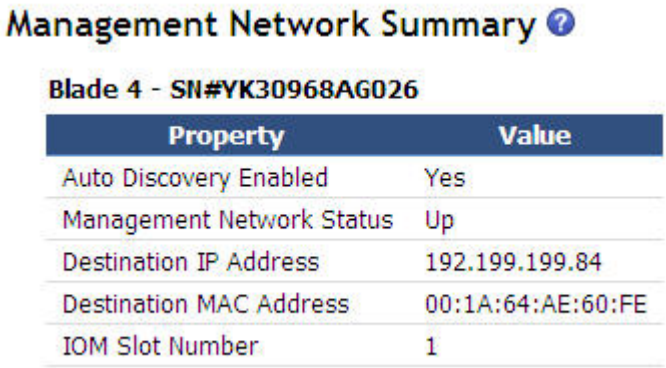
Click **Blade Tasks → Blade Power / Restart** to view the statues of the management network connection for the blade server.



Management network status is shown in the **Management Network** column and has the following states:

-  - indicates that the management path between the blade server and advanced management module is operational.
-  - indicates that the management path between the blade server and advanced management module is not operating.
- No icon indicates that the blade server does not support the display of detailed management network status information.

Click on a management network status icon to display the detailed management network status information for a blade server, similar to what is shown in the following illustration.



IBM Service Advisor

The BladeCenter Service Advisor can automatically send hardware service information to IBM.

Note: Although Service Advisor can send alerts 24 hours a day, 7 days a week, your service provider will respond according to the arrangement that you have in place with them. Please contact them if you have any questions.

The following topics provide instructions for setting up, testing, and maintaining the Service Advisor.

- "Configuring Service Advisor"
- "Using Service Advisor" on page 78
- "Connectivity security for Service Advisor" on page 80

Detailed descriptions of the Service Advisor web interface are in Chapter 3, "Service Advisor" on page 188.

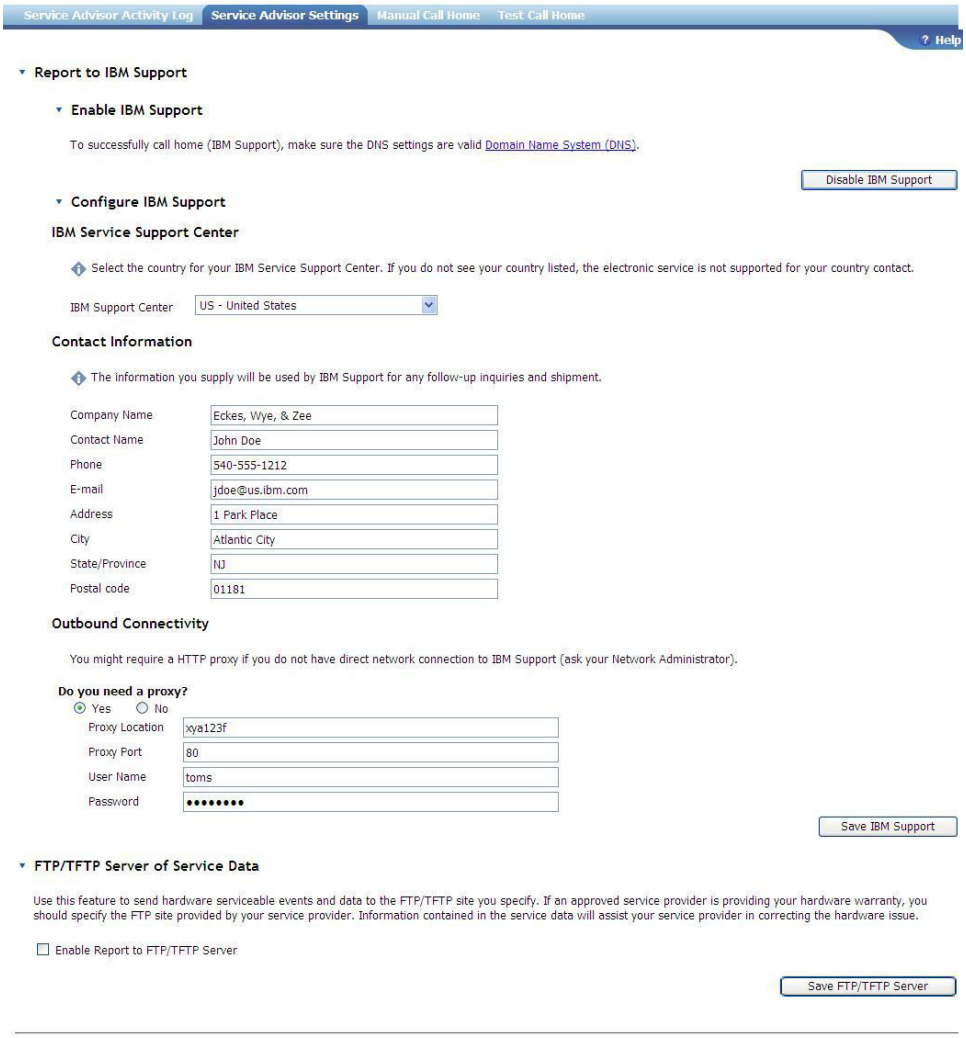
Configuring Service Advisor

You can set up the BladeCenter Service Advisor to automatically send hardware service information to IBM.

To configure the BladeCenter Service Advisor, complete the following steps:

1. Log in to the management module on which you want to activate the Service Advisor. For more information, see "Starting the management-module web interface" on page 11.
2. In the navigation pane, click **Service Tools → Service Advisor**. If this is the first time you select this option, or if the management module firmware was reset to the default values, you will need to view and accept the license agreement.
   a. Click **View terms and conditions** to view the Service Advisor agreement.
   b. Click **I accept the agreement** on the terms and conditions page to close the page.

   Notes:
   - The Call Home feature is disabled by default, and will connect to IBM Support only when enabled.
   - The Call Home feature transmits data that includes BladeCenter unit inventory and status. To download this information to a local file, see "AMM Service Data" on page 184.
   - Service data included in a Call Home report will be used for debugging purposes according to the Terms and Conditions that were accepted prior to before enabling Service Advisor. The link to **View Terms and Conditions** is on the main **Service Advisor** page.
   - None of the information in the Call Home report contains client data from the servers or the I/O modules.
3. Click the **Service Advisor Settings** tab to define the contact information. A page similar to the one in the following illustration is displayed. In this illustration, the fields contain sample entries.



4. Click **Enable IBM Support**. The Service Advisor Activity Log page now displays two additional tabs, **Manual Call Home** and **Test Call Home**.
5. Click the **Service Advisor Settings** tab and fill out the contact information fields.

IBM Service Support Center
Use this dropdown list to select the country for your IBM Service Support Center. If you do not see your country listed, the electronic service is not supported for your country contact.

Company Name
Use this field to indicate the company or organization that controls the management module. This field can contain a maximum of 60 characters.

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

Phone Use this field to indicate the contact phone number.

E-mail Use this field to indicate the email address of the person responsible for the management module.

Address
Use this field to indicate the street address of the company or organization that controls the management module.

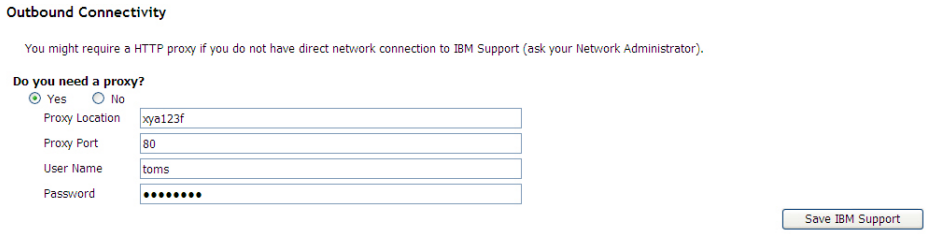
City Use this field to indicate the city of the company or organization that controls the management module.

State/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.

Postal code
Use this field to indicate the postal code.

Outbound connectivity
Use the radio button in this section to indicate whether or not you need to use a proxy.

6. Click **Save**. The Service Advisor page is displayed.
7. If your BladeCenter unit needs to use an HTTP proxy, fill in the Proxy Location, Proxy Port, User Name, and Password fields.



Notes:

- The proxy server will enable the advanced management module to call home from behind some firewalls.
- The proxy server must support connections to port 443 and port 80.
- All communications with IBM Support are handled through TCP sockets that are originated by the advanced management module, and use SSL to encrypt the data that is being sent and received.

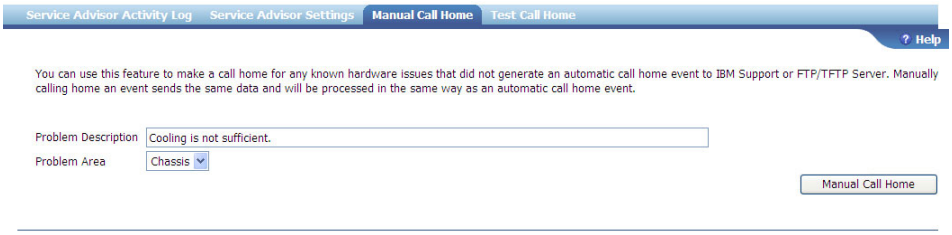
8. Select **Enable Report to FTP/TFTP Server** to send hardware serviceable events and data to the FTP/TFTP site that you specify. If this feature is enabled, fill in the additional configuration fields that are exposed; then, click **Save FTP/TFTP Server**.

Using Service Advisor

After the BladeCenter Service Advisor is set up, you can view the activity log or generate a test message.

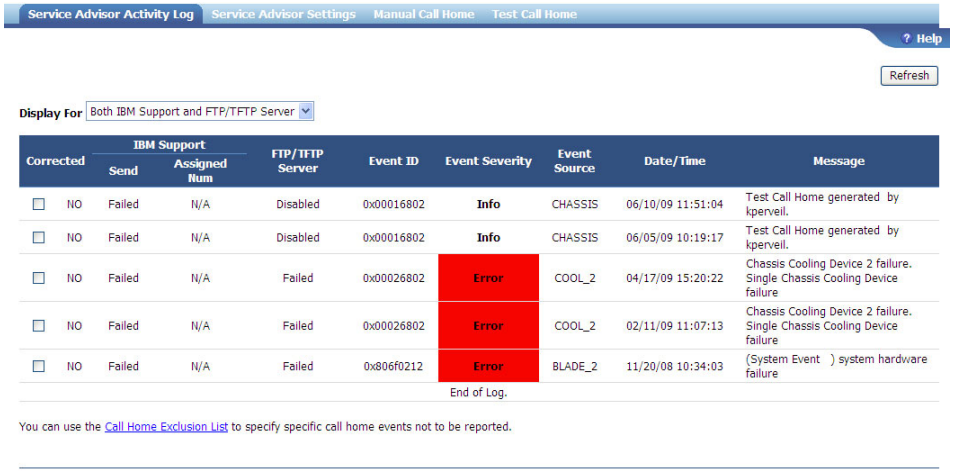
Complete the following steps to create a hardware problem report concerning your BladeCenter unit, or one of its installed blade servers.

1. Log in to the management module on which you want to activate the Service Advisor. For more information, see “Starting the management-module web interface” on page 11
2. In the navigation pane, click **Service Tools → Service Advisor**.
3. Click the **Manual Call Home** tab. You will see a page similar to the following illustration.



4. Complete the following steps.
   a. Select the problem area from the dropdown list.
   b. Enter the problem description.
   c. Click **Manual Call Home**.

   Note: If you would like to send service data using email, use the **Manually Email Service Information** feature of the event log management option. See “Event Log” on page 99.
5. To generate a test message, click the **Test Call Home** tab and the **Test Call Home** push button. The Test Call Home is used to ensure that the advanced management module can successfully call home problems to IBM. Clicking **Test Call Home** will take you to the **Service Advisor Activity Log**. Click the **Refresh** push button on the activity log until a success or failure is registered in the **Send Result** column of the activity log. If the call was successful an Assigned Service Number or ticket number will be assigned. The ticket that is opened at IBM will be identified as a test ticket. No action is required from IBM support for a test ticket, and the call will be closed. If the test call home fails, refer to the “Connectivity security for Service Advisor” on page 80.
6. To view the activity log, click the **Service Advisor Activity Log** tab.



Note:

- The activity log shows the 5 most recent call home events including Test Call Home and Manual Call Home events.
- The Send Result can be Success, Pending, or Failed.
  - Success -- The call was successfully received at IBM. The Assigned Service Number field will include a problem ticket number.
  - Pending -- The call home is in progress.
  - Failed -- The call home failed. In the case of a call home failure, contact IBM to report the hardware service event. Failed call home events will not be retried.

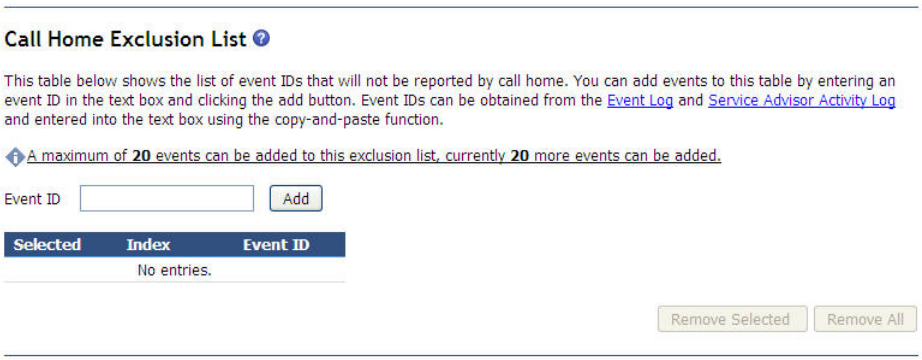
7. Click the **Corrected** checkbox after you resolve each event, to make unresolved events easier to find.

   Note: If the **Corrected** checkbox is not checked for an event, the next occurrence of the same event will be not called home until after five days have passed since the first occurrence of the event.

8. Click the **Refresh** push button to display the latest information. The Assigned Service Number can be used to reference the call home event when communicating with IBM.

   Note: To download the service data, including the service log, see "AMM Service Data" on page 184.

9. To keep a specified event out of the report to IBM, click the Call Home Exclusion List link.



Notes:

- Before using the Call Home Exclusion feature, contact IBM support.
- For a list of the Service Advisor call-home messages, see the *Advanced Management Module IBM BladeCenter Service Advisor Messages Guide.*

10. Enter the hexadecimal Event ID into the Event ID field.
11. Click **Add**.

Connectivity security for Service Advisor

This section describes data that is exchanged between the advanced management module and the IBM Service Center and the method for this exchange. This is limited to the configuration and use of Call Home (Service Advisor) on the advanced management module for automatic error reporting.

The advanced management module can be configured to send service information data back to IBM. By default the call home function is disabled. Service Advisor requires a set of parameters and contact information to enable the call home function.

Service Advisor only connects to IBM when it is enabled for reporting problems and a problem is encountered. The data is transmitted in a service data capture file that includes inventory and status information. To save and view a service data capture file, see "AMM Service Data" on page 184.

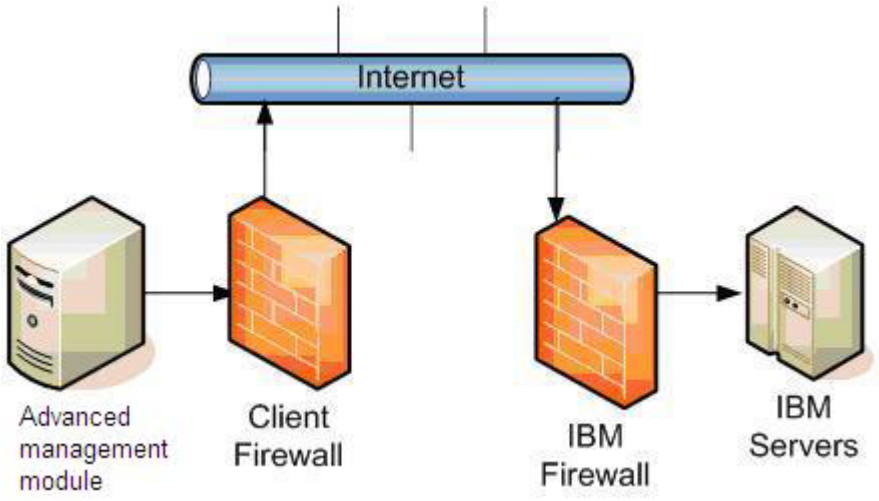
The service data capture file is a .tgz (GZipped Tar Archive) file which you can unbundle using common utilities. The categories of data collected remains the same, while the following details of the data can vary:

- Firmware versions can change.
- Installed components can change.
- Once the logs reach capacity, older information is overwritten by more recent events.
- Exact format and content of the reportable data captured can change.

Note: None of the information or debug data sent to IBM contains client data from the blade servers or I/O modules.

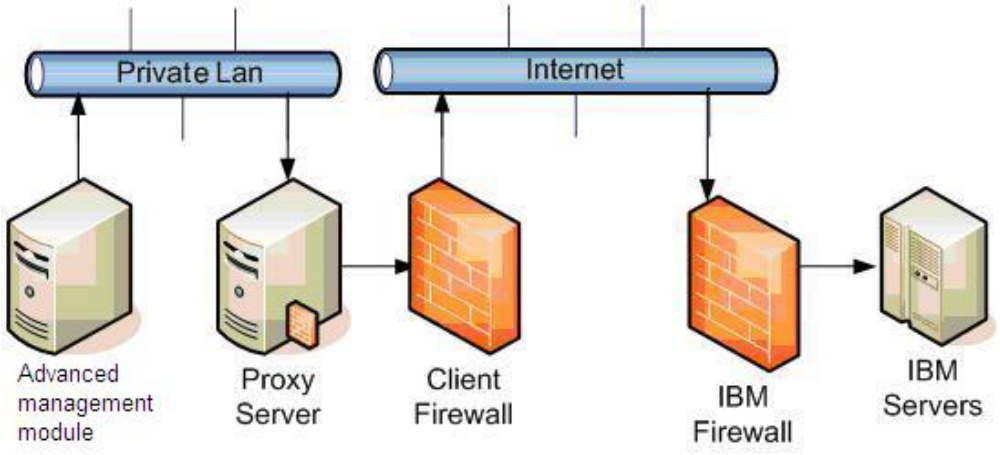
When Service Advisor is enabled, the advanced management module uses a client-provided internet connection to connect to IBM Support. All the communications are handled through TCP sockets, which always originate from the advanced management module, and use SSL to encrypt the data that is being sent back and forth. The advanced management module can be enabled to connect to the Internet through a client-configured proxy server.

The following diagram shows the advanced management module connecting to IBM without a proxy server.



In this setup, the advanced management module connects through the client-provided Internet connection by the default route. For the advanced management module to communicate successfully, your external firewall must allow established TCP packets to flow freely on port 443 (HTTPS).

The following diagram shows the advanced management module connecting to IBM using a client-provided proxy server.



To forward SSL sockets, the proxy server must support the basic proxy header functions (as described in RFC 2616, Hypertext Transfer Protocol 1.1; see http://www.ietf.org/rfc/rfc2616.txt) and the connect method. Basic proxy authentication (RFC 2617, HTTP Authentication: Basic and Digest Access Authentication; see http://www.ietf.org/rfc/rfc2617.txt) can be configured so that the advanced management module authenticates before attempting to forward sockets through the proxy server.

For the advanced management module to communicate successfully, the client's proxy server must allow connections to port 443 and port 80. The proxy server can also limit the specific IP addresses to which the advanced management module can connect.

When the advanced management module with Service Advisor enabled detects a problem for itself or one of the BladeCenter components, a problem report will be called home to IBM. All the information in that report will be temporarily stored. Once the transmission is complete, the advanced management module will no longer provide status information for the opened call. IBM Support will contact you to perform additional problem determination and find a solution. Support Engineers that are actively working on a problem can offload the data for debugging purposes and then delete it when finished.

Some or all of the following IPv4 IP addresses are used by the advanced management module when it is enabled. Both HTTP (port 80) and HTTPS (port 443) are required.

Note: These IP addresses are subject to change.

- www6.software.ibm.com, 207.25.253.41
- www.ecurep.ibm.com, 192.109.81.20
- download2.boulder.ibm.com, 207.25.253.8
- download3.boulder.ibm.com, 207.25.253.76
- www-945.ibm.com, 129.42.26.224
- www-945.ibm.com, 129.42.34.224
- www-945.ibm.com, 129.42.42.224
- eccgw01.boulder.ibm.com, 207.25.252.197
- eccgw02.rochester.ibm.com, 129.42.160.51
- testcase.boulder.ibm.com, 207.25.253.31

To verify connectivity from the advanced management module to IBM, point your browser to one of the addresses in the above list. If connectivity is successful then an IBM web page will bedisplayed. Note that the addresses beginning with eccgw cannot be browsed.

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.
- IPv6 addressing is not supported by all I/O modules.
- The I/O Module web interface is supported only by Microsoft Internet Explorer version 8 or later and Mozilla Firefox version 1.07 or later.

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: For IPv4, 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.

NEBS mode support

BladeCenter T and BladeCenter HT units support Network Equipment-Building System (NEBS) mode.

If you are operating a BladeCenter T or BladeCenter HT unit in a NEBS (Telco) environment, you must enable NEBS mode by selecting the **Network Equipment-Building System (NEBS) mode** check box in the **BladeCenter Chassis Configuration Setting** section of the **Monitors → Power Management** page (see "Power Management" on page 106 for additional information).

In a NEBS environment, the fans in the BladeCenter unit do not speed up as readily in response to potential thermal events as in a non-NEBS environment. To enable acoustic mode for the BladeCenter unit, which reduces blade server power consumption to stay within acoustic noise limits, you must disable NEBS mode.

Air filter management for BladeCenter HT and BladeCenter T units

The BladeCenter HT and BladeCenter T units provide alarms and reminders relating to air filter condition.

The air filters on the BladeCenter HT and BladeCenter T units must be changed on a regular basis. Depending on your BladeCenter unit type, the air filter alarms and reminders might be cleared automatically.

Fouled-filter detection

BladeCenter T and BladeCenter HT units warn you when the air filter is clogged.

The advanced management module generates the air filter alarm (minor, major, or critical) according to the severity of the clogging of the air filter panel in the front bezel. These alarms can be viewed in the **Monitors → System Status** page and appear in the management module event log (see "System Status" on page 91 and "Event Log" on page 99 for more information).

The BladeCenter HT unit does not require you to manually manage air filter alarms, because the filter in this BladeCenter unit is automatically detected and fouled-filter detection is enabled when the front bezel is installed. When the front bezel is removed, fouled-filter detection is automatically disabled, and no fouled-filter alarm is created. The fouled-filter alarm is automatically reset when the front bezel is reinstalled on the BladeCenter HT unit.

The BladeCenter T unit requires you to manually manage fouled-filter configuration settings, because it cannot detect the installation or removal of the front bezel. Fouled-filter detection is enabled, disabled, or reset as part of the air filter reminder configuration in the **Passive Air Filter Reminder** section of the **MM**

Control → Alerts page (see "Alerts" on page 160 for more information). Alarms for a fouled filter must be manually cleared in the **Major Alarms** or **Minor Alarms** sections of the **Monitors → System Status** page (see "BladeCenter T and BladeCenter HT alarm management" on page 92 for information and instructions).

Passive air filter reminder

BladeCenter T and BladeCenter HT units remind you to change the air filter every six months.

A service reminder to change the air filter in a BladeCenter T or BladeCenter HT unit is generated every six months. These reminders appear as information messages in the management module event log (see "Event Log" on page 99 for information about using the Event Log).

The BladeCenter HT unit automatically generates an event to remind you to change the air filter when six months have elapsed after the advanced management module has detected that you have removed and then installed the front bezel. The BladeCenter HT unit automatically detects and responds to the following conditions relating to air filter management:

Insertion
The six months of service and the fouled-filter detection schedules start when the front bezel is installed on the BladeCenter HT unit.

Removal
No filter management services are available when the front bezel is removed from the BladeCenter HT unit.

The BladeCenter T unit provides controls in the advanced management module user interface so that you can reset the service interval, because this BladeCenter unit does not detect front bezel activity. Six months after you reset the service interval in the advanced management module user interface, you receive a reminder to change the air filter in the front bezel.

The BladeCenter T provides the following air filter management options in the **Passive Air Filter Reminder** section of the **MM Control → Alerts** page (see "Alerts" on page 160 for more information):

- **Disable**: Air filter management services are turned off (no air filter alarms or events are generated).
- **Enable**: The six months of service reminder schedule and fouled-filter detection are turned on.
- **Restart**: Air filter management services are reset (six months of service reminder schedule is set to generate an air filter reminder in six months).

Chapter 3. Management-module web interface overview

The following topics contain information about the structure and content of the management-module web interface for all management-module types:

- 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" on page 88)
- Descriptions of the management-module web interface pages (see "Management-module web interface options" on page 91)

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.
- Configuring security settings such as data encryption and user account security.
- Selecting recipients for alert notification of specific events.
- Monitoring the status of the BladeCenter unit, blade servers, and other BladeCenter components.
- Discovering other BladeCenter units on the network and enabling access to them through their management-module web interfaces.
- 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 units only).

You also can use the management-module web interface, SNMP, SMASH, 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

	Role required to change information or execute tasks										
Page	**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**
Monitors											
System Status	•	•	•	•	•	•	•	•	•	•	•
Event Log (view)	•	•	•	•	•	•	•	•	•	•	•
Event Log (clear or set log policy)	•							•			

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**
LEDs	•	•	•		•	•	•	•	•	•	•
Power Management	•	•	•		•	•	•	•	•	•	•
Hardware VPD	•	•	•		•	•	•	•	•	•	•
Firmware VPD	•	•	•		•	•	•	•	•	•	•
Remote Chassis	•			•	•						
Blade tasks											
Power/Restart	•					•					
Remote Control (remote console)	•		•								
Firmware Update	•					•					
Configuration	•									•	
Advanced Configuration (blade bay data)	•										
Serial Over LAN	•								•	•	
Open Fabric Manager	•										
I/O-module tasks											
Admin/Power/Restart	•						•				
Configuration (see Note 1)	•										•
Firmware Update	•						•				
Storage tasks											
Configuration	•								•		
MM control											
General Settings	•								•		
"Login Profiles" on page 151 (account security management)	•	•									
"Alerts" on page 160 (see Note 2)	•								•		
Serial Port	•								•		
Port Assignments	•								•		
Network Interfaces	•								•		
Network Protocols	•								•		
Chassis Internal Network	•										
Security	•								•		

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**
Configuration Mgmt (backup configuration to file)	•	•		•	•			•	•		
Configuration Mgmt (save configuration to BladeCenter unit)	•										
Configuration Mgmt (restore)	•										
Configuration Mgmt (Config Wizard)	•										
File Management	•				•	•	•		•	•	•
Firmware Update	•				•						
Restart MM	•				•						
"License Manager" on page 181	•				•						
Service tools											
AMM Service Data (view only) See Note 4.		•			•			•	•		
Blade Service Data Only applies to some blade servers.	•										
AMM Status (view only)											
Service Advisor (see Note 5)	•								•		
"Scalable Complex" on page 190	•									•	

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.
4. To view AMM service data, the Chassis User Account Management, Chassis Administration, Chassis Log Administration, and Chassis Configuration roles are required.

5. To perform a **Service Advisor Manual Call Home** or **Test Call Home**, the Chassis configuration, Chassis administration, Blade configuration, Blade administration, I/O module configuration, or I/O module administration role is 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. For the advanced management module, web interface pages are date and time stamped each time that they are refreshed.

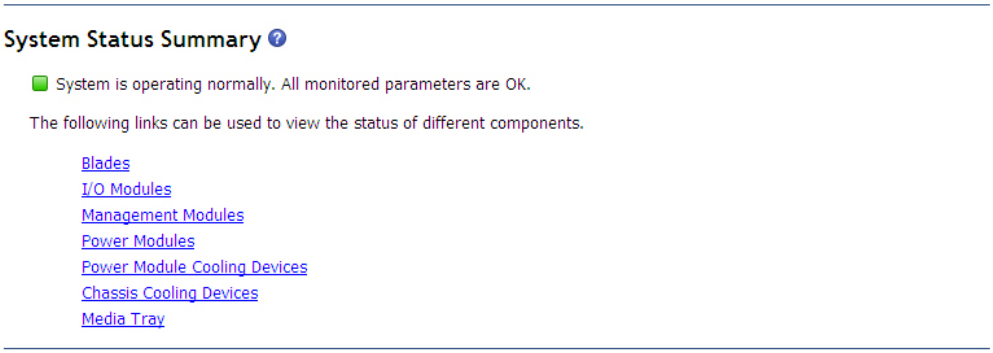
Monitors

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

System Status

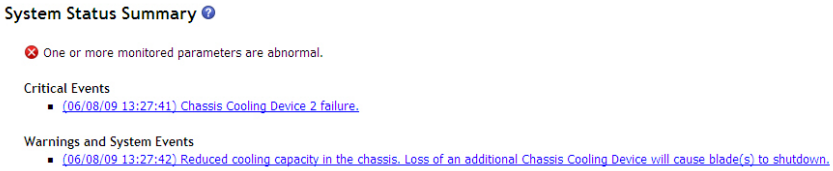
Select **Monitors → System Status** to view the overall system status, a list of outstanding events that require immediate attention, and the overall status of each of the blade servers and other components in the BladeCenter unit.

The following page is displayed.



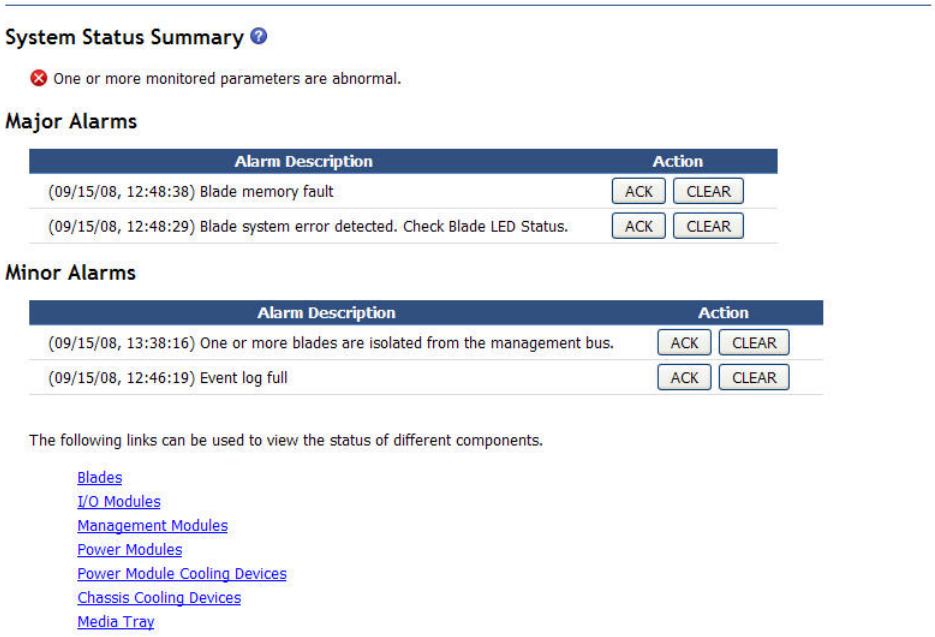
Note: The BladeCenter S unit includes a link for **Storage Module** status.

If an abnormal system condition is detected, it is shown in the system status summary along with the date and time that the condition occurred and a link to additional information. Clicking on an event link displays detailed event information and recommended actions. (See the *BladeCenter Advanced Management Module Messages Guide* for a complete list of all non-device specific events and recommended actions, sorted by event ID. Device specific event information is in the documentation for the device.) The following illustration shows the system status summary with an abnormal event.



BladeCenter T and BladeCenter HT alarm management:

Select this page to manage alarms for the BladeCenter T and BladeCenter HT units.



For the BladeCenter T and BladeCenter HT units, 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 a BladeCenter T or BladeCenter HT 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 for the advanced management module.

Blades

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

Bay	Status	Name	Pwr	Owner**		cKVM*	I/O Compatibility	WOL*	Local Control			BEM*
				KVM	MT*				Pwr	KVM	MT*	
1	D	Discovering	---				OK	---	•	•	•	---
2		*No blade present*										
3	D	Discovering	---				OK	---	•	•	•	---
4		*No blade present*										
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*										

* MT = Media Tray (CD/ USB) , WOL = Wake on LAN , BEM = Blade Expansion Module
BSE1 (BSE2,BSE3) = Blade Storage Expansion 1st Generation (2nd Generation, 3rd Generation)
PEU1 = PCI Expansion Unit 1st Generation PEU2 = PCI Expansion Unit II BPE3 = PCI Express Expansion Unit
cKVM = Concurrent KVM BIE = Blade I/O Expansion BPR = Blade Processor 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 blade server. 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 advanced 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.

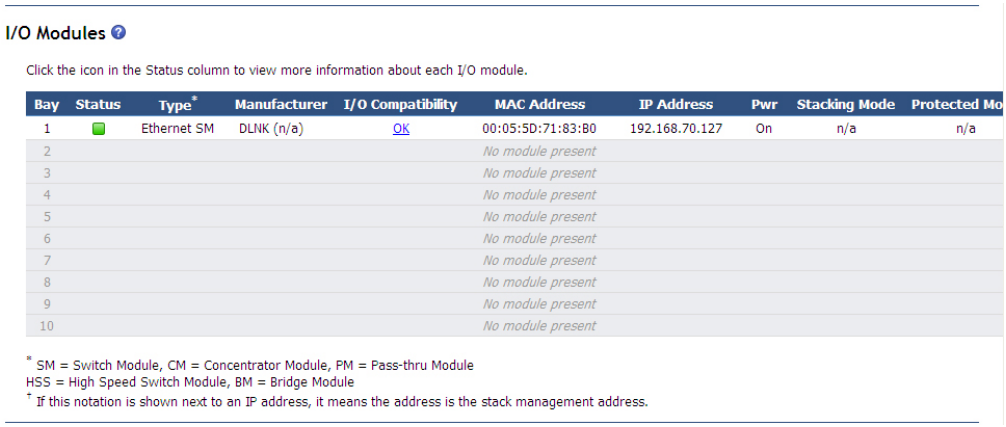
- **Owner**: An indication of whether the current blade server controls the following BladeCenter resources:
  - **KVM:** Keyboard, video, and mouse
  - **MT:** The media tray that contains the removable-media drives and USB ports

  Note: The advanced management module has two USB ports. If you connect a USB storage device to one, blade servers in the BladeCenter unit also can use it. The rules that determine which blade server detects the USB storage device are as follows:

  1. For the BladeCenter unit, the USB storage device mounts to the blade server that has ownership of the KVM.
  2. For the BladeCenter H or HT unit, the USB storage device mounts to the blade server that has ownership of the media tray.
  3. The management modules for the BladeCenter T unit do not have USB ports.
- **cKVM**: Shows whether a concurrent KVM (cKVM) feature card is installed in the blade server.
- **I/O Compatibility**: The compatibility status of the blade server. Each status is a link to detailed compatibility information for the blade server.
- **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 122 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 for an advanced management module.


I/O Modules

Click the icon in the Status column to view more information about each I/O module.

Bay	Status	Type*	Manufacturer	I/O Compatibility	MAC Address	IP Address	Pwr	Stacking Mode	Protected Mo
1		Ethernet SM	DLNK (n/a)	OK	00:05:5D:71:83:B0	192.168.70.127	On	n/a	n/a
2					No module present				
3					No module present				
4					No module present				
5					No module present				
6					No module present				
7					No module present				
8					No module present				
9					No module present				
10					No module present				

* SM = Switch Module, CM = Concentrator Module, PM = Pass-thru Module
HSS = High Speed Switch Module, BM = Bridge Module
* If this notation is shown next to an IP address, it means the address is the stack management address.

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

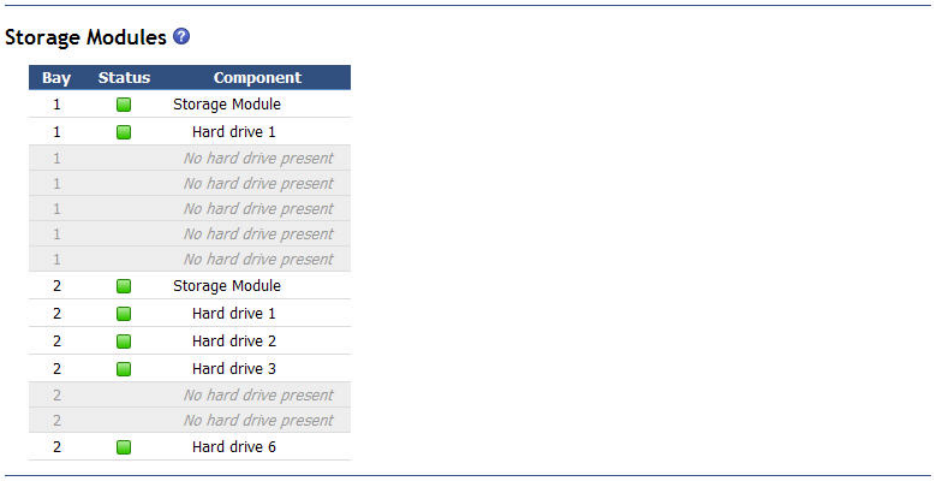
- **Bay**: The number of the bay that the I/O module occupies.
- **Status**: An icon that indicates good , warning , or critical status for the I/O module Click this icon to view detailed I/O module compatibility information.
- **Type**: The type of I/O module in the bay, such as an Ethernet I/O module, Fibre Channel I/O module, or pass-thru module.
- **Manufacturer**: The I/O module manufacturer.
- **I/O Compatibility**: The compatibility status of the I/O module. Each status is a link to detailed compatibility information for the I/O module. For some I/O modules, clicking the status link will display detailed status information for the I/O module ports.
- **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.

  Notes:
  - Some types of I/O modules, such as a pass-thru module, do not have a MAC address or an IP address.
  - The RAID SAS module, available on the BladeCenter S, requires and displays two MAC addresses and two IP addresses.
- **IP Address**: The IP address of the I/O module.
- **Pwr**: The power state (on or off) of the I/O module.
- **Stacking Mode**: The stacking mode status of the I/O module.
- **Protected Mode**: The current protected mode status of the I/O module.
  - **n/a**: Protected mode capability does not exist on the I/O module.
  - **Disabled**: Protected mode capability exists on the I/O module but has not been activated on the I/O module or the advanced management module.
  - **Pending**: Protected mode has been activated on the advanced management module but not yet on the I/O module.

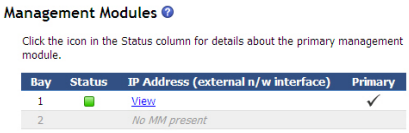
  - **Active**: Protected mode is active on both the I/O module and the advanced management module.
  - **Attention**: Protected mode is enabled on the I/O module but not on the advanced management module.
- **POST Status**: Text information about the status of the I/O module.

In the BladeCenter S unit, the advanced management module provides a link to the **Storage Modules** page that displays the following information.



- **Bay**: The bay number of each installed storage module.
- **Status**: An icon that indicates good , warning , or critical status of the storage module.
- **Component**: The type of component that is contained in this storage module.

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 management module. 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. For the advanced management module, the detailed status will also display a list of users who are logged in to the management module along with their access information. A **Terminate** push button is shown for each user who is logged in to the advanced management module at the time this page was generated. If a user does not have system administrator authority, the button is enabled only for that user's sessions.
- **IP Address**: Clicking **View** displays IP address information for 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.

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

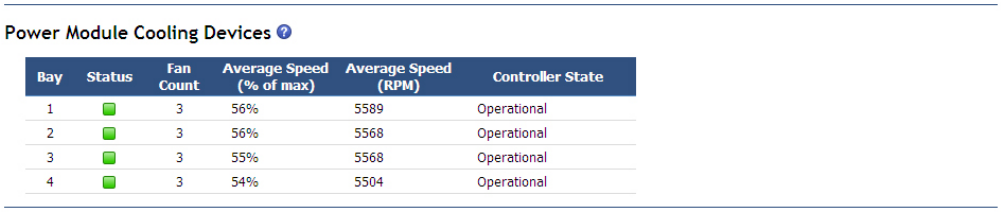

Power Modules

Bay	Status	Details
1		Power module status OK
2		Power module status OK
3		Power module status OK
4		Power module status OK

- **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.
- **Details**: Text information about the status of the power module.

Note: When an advanced management module is installed in a BladeCenter S unit, a line under the Power Modules table indicates whether the BladeCenter unit is connected to a 110 V ac or 220 V ac power source.

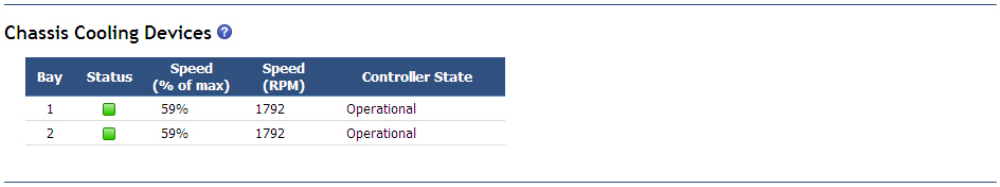
When you click **Power Module Cooling Devices** (some BladeCenter units support this feature), the following information is displayed:


Power Module Cooling Devices

Bay	Status	Fan Count	Average Speed (% of max)	Average Speed (RPM)	Controller State
1		3	56%	5589	Operational
2		3	56%	5568	Operational
3		3	55%	5568	Operational
4		3	54%	5504	Operational

- **Bay**: The number of the power module bay that the power-module cooling device occupies.
- **Status**: An icon that indicates good , warning , or critical status of the power-module cooling device.
- **Fan Count**: The number of fans in the power-module cooling device that are operational.
- **Average Speed (% of max)**: The current speed of the power-module cooling device, as a percentage of the maximum revolutions per minute (rpm). The power-module cooling device speed varies with the thermal load. An entry of `Offline` indicates that the power-module cooling device is not functioning.
- **Average Speed (RPM)**: The current speed of the power-module cooling device, in rpm. The power-module cooling device speed varies with the thermal load.
- **Controller State**: The status of the power-module cooling device speed controller: operational, flashing (firmware is updating), not present, or communication error.

When you click **Chassis Cooling Devices**, the following information is displayed:


Chassis Cooling Devices

Bay	Status	Speed (% of max)	Speed (RPM)	Controller State
1		59%	1792	Operational
2		59%	1792	Operational

- **Bay**: The number of the bay that the BladeCenter unit cooling device module occupies.
- **Status**: An icon that indicates good , warning , or critical status of the BladeCenter unit cooling device.
- **Speed (% of max)**: The current speed of the BladeCenter unit cooling device module, as a percentage of the maximum revolutions per minute (rpm). The BladeCenter unit cooling device speed varies with the thermal load. An entry of `Offline` indicates that the BladeCenter unit cooling device is not functioning.
- **Speed (RPM)** (advanced management module installed in a BladeCenter H unit only): The current speed of the BladeCenter unit cooling device module, in rpm. The BladeCenter unit cooling device speed varies with the thermal load.
- **Controller State** (advanced management module installed in a BladeCenter H unit only): The status of the blower speed controller: operational, flashing (firmware is updating), not present, or communication error.

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


Media Tray

Bay	Temp (°C)	Warning	Warning Reset
1	23.00	39.00	30.00

- **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.
- **Hysteresis** (advanced management module installed in a BladeCenter T unit only): The difference between the warning and the warning reset temperature thresholds.

Event Log

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

The event log page includes entries for system events, which are detected by the BladeCenter unit and installed components, and for audit events, which are generated by users. The event log page displays the most recent entries first. Information about all remote access attempts and changes to the advanced management module configuration settings are recorded in the audit log, and the management module sends out the applicable alerts if it is configured to do so. The event log is of fixed capacity. When the log is full, new entries overwrite the oldest entries. On the BladeCenter T or BladeCenter HT unit, when the log is full, the BladeCenter T or BladeCenter HT MNR (minor 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 page and suppress the display of event IDs that link to event information; clicking on an event ID link displays detailed event information and recommended actions, when appropriate. See the event log help for more information. See the *BladeCenter Advanced Management Module Messages Guide* for a complete list of all non-device specific events and recommended actions, sorted by event ID. Device specific event information is in the documentation for the device.

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

- BladeCenter unit (SERVPROC)
- Blade device by bay number (Blade_*xx*)
- Operator actions (Audit)
- Storage module by bay number (Stor_*xx*)
- I/O module by bay number (IOMod_*xx*)
- Cooling device by number (Cool_*xx*)

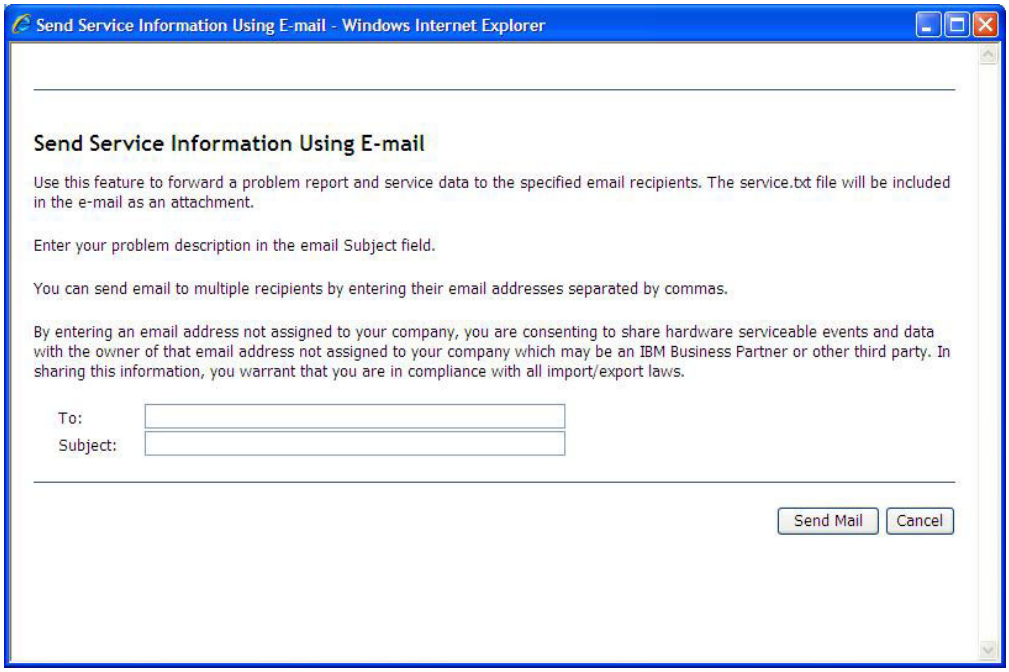
- Power module by number (Power_*xx*)

Notes:

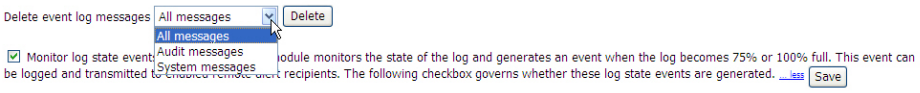
- *xx* in an event source refers to the bay number of the reporting device.
- Events that trigger alarms on the Blade Center T unit send alerts to the advanced management module. Alerts are assigned severity ratings of Error, Warning, and Information. Critical and major events are written to the log as errors, and minor events are written as warnings.

Select the **Call Home** checkbox to see which events are serviceable. Serviceable events are usually triggered by hardware or firmware issues. If you have activated the Service Manager feature (see "Configuring Service Advisor" on page 75), these events will be automatically reported.

You also can click the **Send service information using e-mail** link to send a snapshot of the event log to a specified email address. This choice will display a popup window, similar to the illustration below, that you can use to specify the email address and purpose of the communication. The SMTP server must be configured to use this feature (see "Network Protocols" on page 170 for information). Click the **Download the log** link to download and save a copy of the event log in comma-separated value (CSV) format.



Messages can be cleared from the event log by choosing the messages to delete and clicking **Delete** at the top of the page. You can also click **Save** to save the combined event log as a text file.



LEDs

Select **Monitors → LEDs** to manage LED behaviors for Telco and other BladeCenter units.

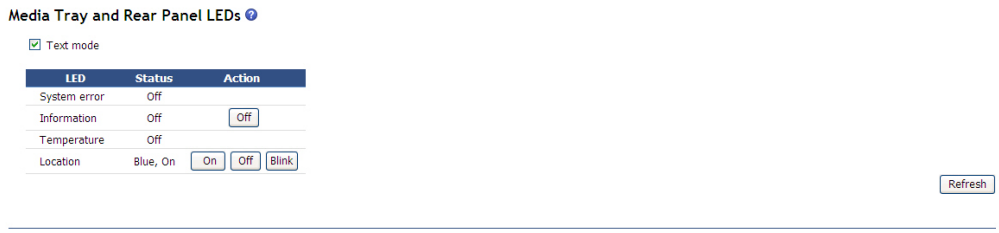
BladeCenter unit LEDs:

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

Note: The BladeCenter S unit includes a link to **Storage LEDs** after the link to I/O module 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. Selecting **Text Mode** indicates device status without using graphic icons.

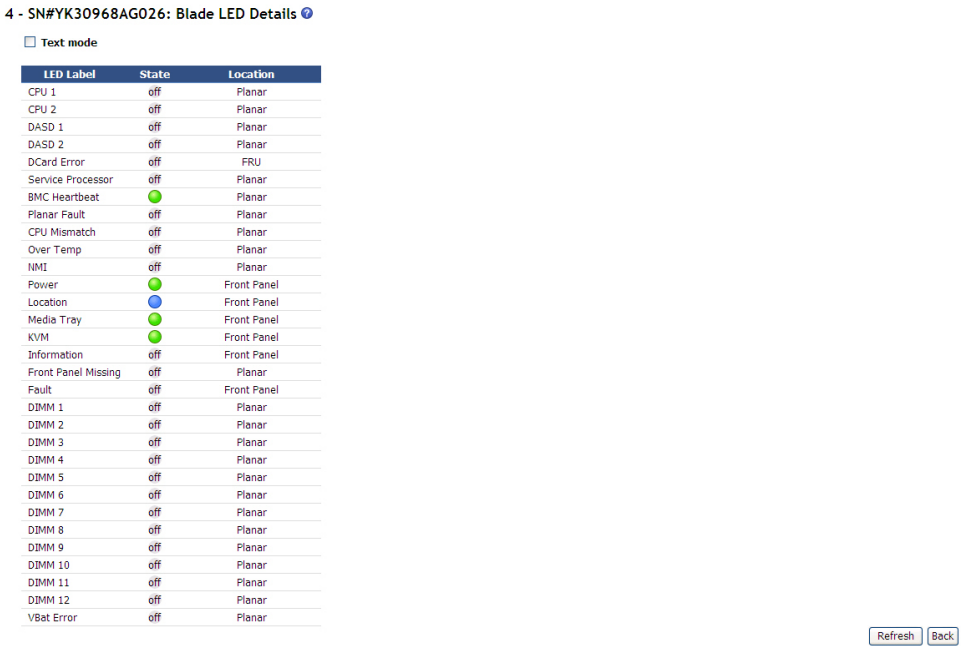
The following information is displayed. (Examples of Media Tray LEDs are shown using both icons and Text Mode.)



- **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**: 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

  For the advanced management module, click the blade server name to view the status of the blade server light path diagnostics LEDs. (The LEDs that are shown vary by blade server type.) The following illustration shows an example of the light path diagnostics LEDs that are shown in a **Blade LED Details** page.

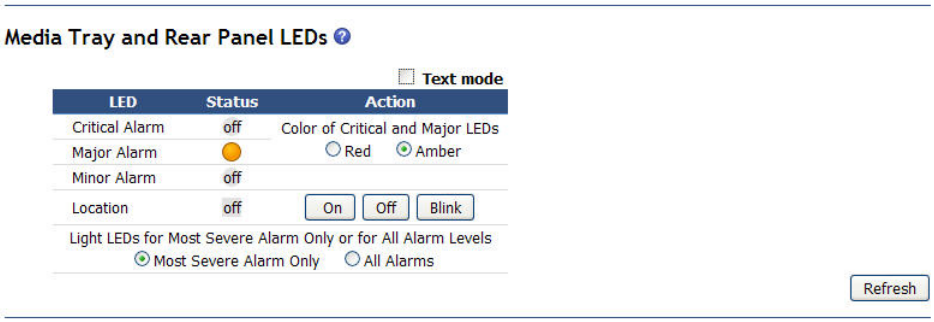


- **I/O-Module LEDs**: The state of the LEDs on some I/O modules. Simulated I/O-module LEDs might also be supported for some I/O modules based on status information that the I/O module maintains, such as port link status, as seen in **I/O Module Tasks → Configuration**. The state of simulated LEDs is inferred from status conditions and does not indicate the state of an actual LED.
- **Storage Unit LEDs**: (BladeCenter S unit only). The state of the storage units.

- **Power module cooling devices LEDs** (advanced management module installed in a BladeCenter H unit only): The state of the error LED on each power-module fan pack.
- **Chassis cooling devices LEDs** (advanced management module installed in a BladeCenter H unit only): The state of the error LED on each BladeCenter unit cooling device.

BladeCenter T and BladeCenter HT alarm management:

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



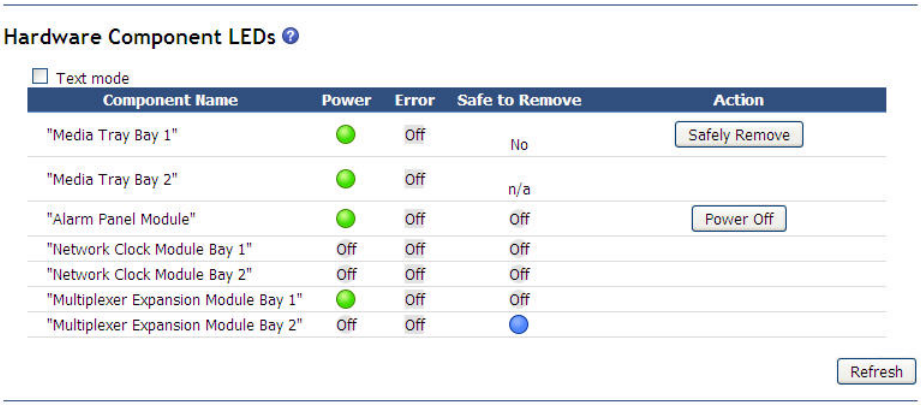
Select **LEDs** to view the state of the BladeCenter T or BladeCenter HT system-status page and blade server control panel LEDs. You also can use this choice to turn on, turn off, or flash the location LED on the BladeCenter unit and the blade servers, and control how the LEDs respond to alarms.

The following information is displayed:

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

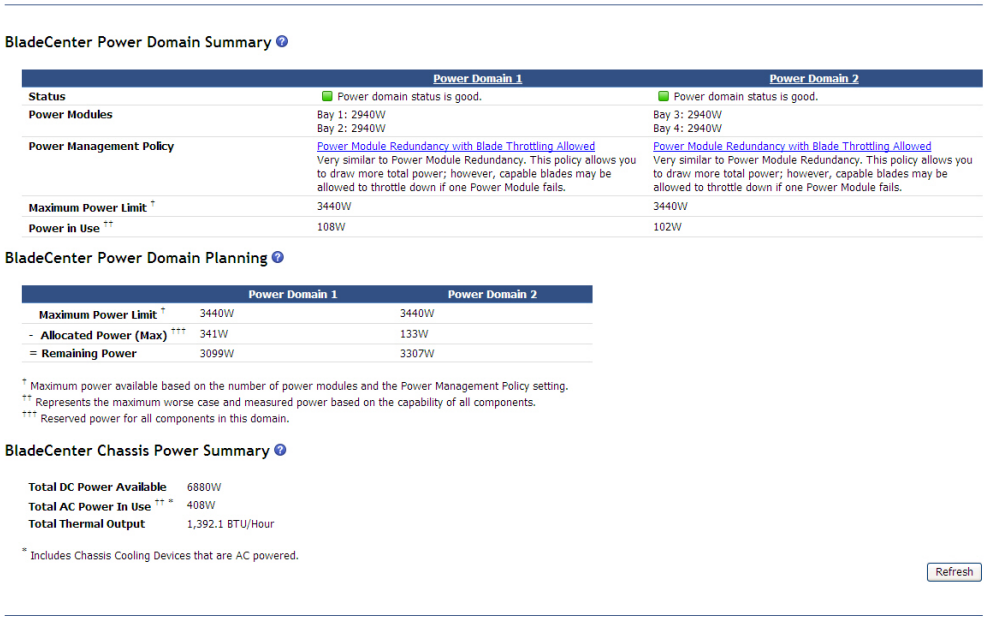
  You can change the state of the location LED and select the active LED color (red or amber) for the critical and major alarm LEDs. This color selection is applied to the LEDs on the front and rear of the BladeCenter T or BladeCenter HT unit and to the LED indications that are shown on this page. You 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 or BladeCenter HT 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 91 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. On BladeCenter HT chassis, you can plug compact flash cards into the media trays to extend the capacity of local storage on the advanced management module. In this way, you can upload larger ISO/image files by using the remote disk feature. To ensure the filesystem integrity on compact flash cards, make the media tray ready for removal by first clicking the **Safely Remove** button. After the **Safe to Remove** message becomes **Yes**, you can remove the media tray. If you change your mind after the media tray becomes Safe to Remove, then you can click the **Re-Enable** push button to remount the file system on the compact flash cards.



Power Management

Select **Monitors → Power Management** to view the power information, based on projected power consumption, for each power domain and to configure power management for the BladeCenter unit.



There are two power domains in most BladeCenter units.

Note: The BladeCenter S unit has one power domain. For a BladeCenter S unit, a table in the **Power Management** page displays only one power domain and contains an additional line to indicate whether the unit is using 110 V ac or 220 V ac power.

Click **Power Domain 1 details** or **Power Domain 2 details** for the list of BladeCenter components in each power domain (see “Detailed power information” on page 109 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 level (throttle) or not turn on.

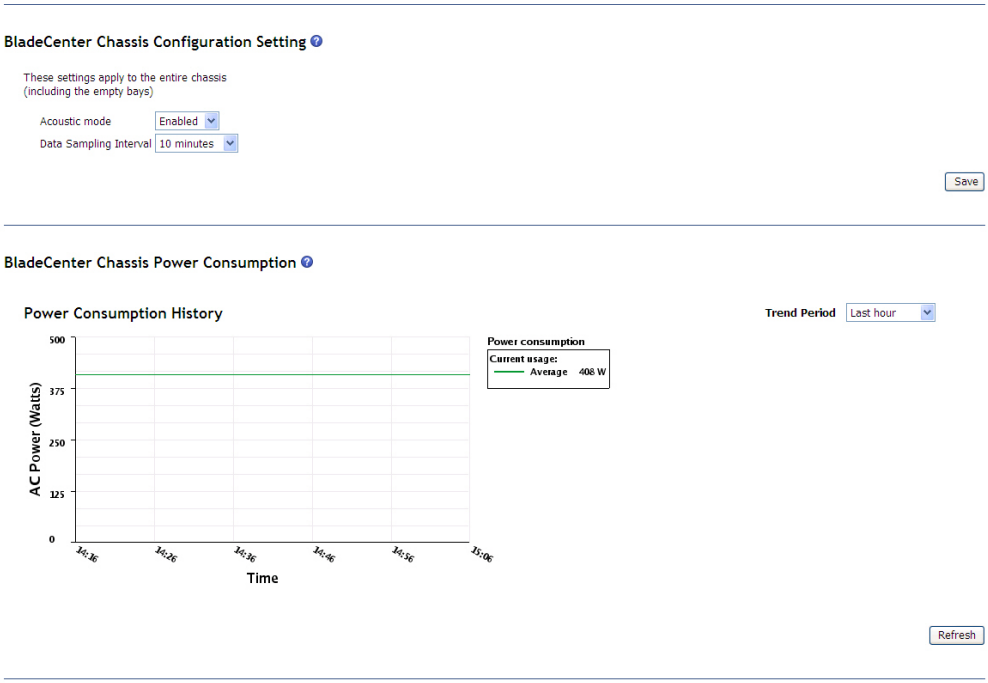
The following power status information is displayed in the **BladeCenter Power Domain Summary**, the **BladeCenter Power Domain Planning**, and the **BladeCenter Chassis Power Summary** sections:

- **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 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 129 for information).
- **Maximum Power Limit**: This field displays the amount of power that is available in each power domain, in watts. Total power is calculated by the advanced 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.
- **Power in Use**: This field displays the current power that is being used in each power domain, in watts. Usually, a module consumes less power than the maximum allocated power. For this reason, the total power that is actually consumed by the chassis might be less than the amount that is shown in this field.
- **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.

  Note: The maximum allocated power for modules is the worst-case amount that the module might consume. The power-in-use number for some modules, including I/O modules, the midplane, and the management module, is the maximum allocated power when the module is powered-on. Usually, a module consumes less power than the maximum allocated power. Therefore, the total power that is actually consumed by the chassis might be less than the amount that is shown in the **Power in Use** field.
- **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.
- **Total DC Power Available**: This field displays the total amount of dc power that is available for the entire BladeCenter unit. It is the sum of the two power domain ratings.
- **Total AC Power In Use**: This field displays the total ac power that is being consumed by all modules in the BladeCenter unit. For BladeCenter H units, it also includes the power that is consumed by the blowers.

- **Total Thermal Output**: This field displays the thermal output (load) of the BladeCenter unit, in Btu per hour. The value is calculated according to the total ac power that is in use.

On this page, you also can configure over-temperature response for the BladeCenter unit, set the power data sampling interval, and view a graph of BladeCenter unit power consumption. You can also enable or disable NEBS operating mode for BladeCenter T and BladeCenter HT units.



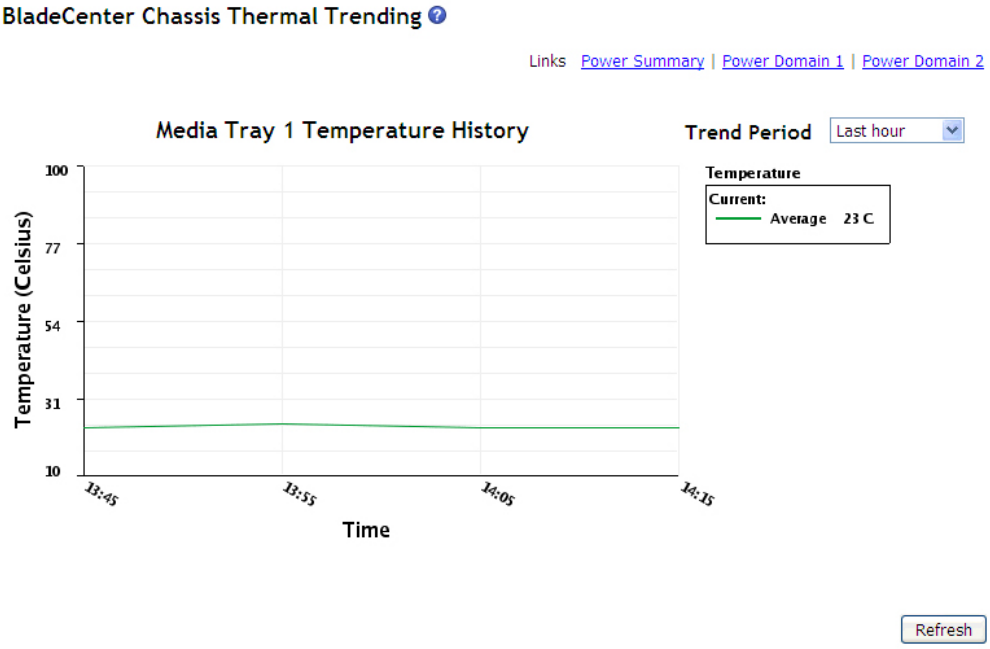
The **BladeCenter Chassis Configuration Setting** section configures how the management module responds if it detects an over-temperature condition (thermal event) on a blade server. The following acoustic mode options are supported in response to thermal events:

- **Network Equipment-Building System (NEBS) mode** check box (BladeCenter T and BladeCenter HT units only): Use this checkbox to enable or disable NEBS mode (see "NEBS mode support" on page 84 for additional information).
- **Acoustic mode**:
  - **Disabled** (default): Increase the blower speeds, as needed, to provide additional cooling.
  - **Enabled**: Reduce blade server power consumption (throttle blade servers) to stay within acoustic noise limits. This option affects only those BladeCenter components that support power throttling.

    Note: To enable acoustic mode for BladeCenter T and BladeCenter HT units, you must disable NEBS mode.
- **Data Sampling Interval**: Determines how often that power information is gathered for trending purposes.

Click the links at the bottom of the page to display thermal trending information for individual BladeCenter components. The components that are monitored and listed vary according to BladeCenter unit type.

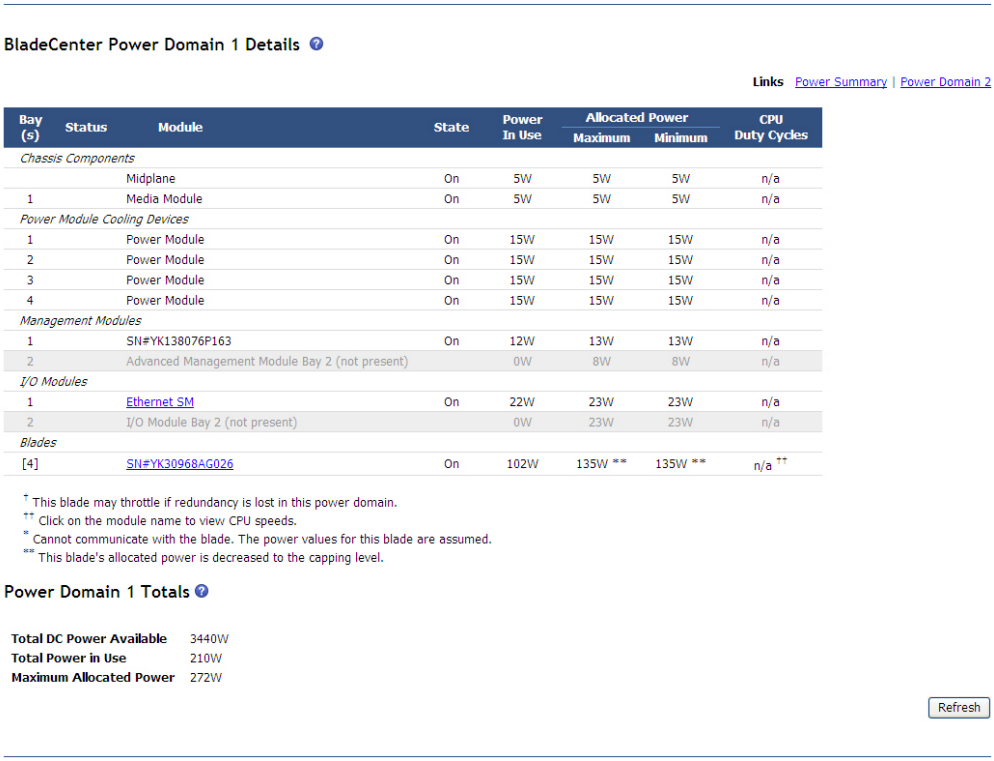
The following illustration shows the media tray temperature information, as an example.



Detailed power information:

Select **Monitors → Power Management → Power Domain Summary** to view detailed power status information for each monitored BladeCenter component.

The BladeCenter components that are part of each power domain are grouped by type. The information for power domain 1 is shown. There is a separate status page for each power domain in your BladeCenter unit. On this page, you also can configure power domain response to loss of power redundancy and view a graph of power consumption for the power domain (similar to the BladeCenter unit power graph). See “Power Management” on page 106.



BladeCenter Power Domain 1 Details

Links Power Summary | Power Domain 2

Bay (s)	Status	Module	State	Power In Use	Allocated Power		CPU Duty Cycles
					Maximum	Minimum	
Chassis Components							
		Midplane	On	5W	5W	5W	n/a
1		Media Module	On	5W	5W	5W	n/a
Power Module Cooling Devices							
1		Power Module	On	15W	15W	15W	n/a
2		Power Module	On	15W	15W	15W	n/a
3		Power Module	On	15W	15W	15W	n/a
4		Power Module	On	15W	15W	15W	n/a
Management Modules							
1		SN#YK138076P163	On	12W	13W	13W	n/a
2		Advanced Management Module Bay 2 (not present)		0W	8W	8W	n/a
I/O Modules							
1		Ethernet SM	On	22W	23W	23W	n/a
2		I/O Module Bay 2 (not present)		0W	23W	23W	n/a
Blades							
[4]		SN#YK30968AG026	On	102W	135W **	135W **	n/a ††

† This blade may throttle if redundancy is lost in this power domain.
†† Click on the module name to view CPU speeds.
* Cannot communicate with the blade. The power values for this blade are assumed.
** This blade's allocated power is decreased to the capping level.

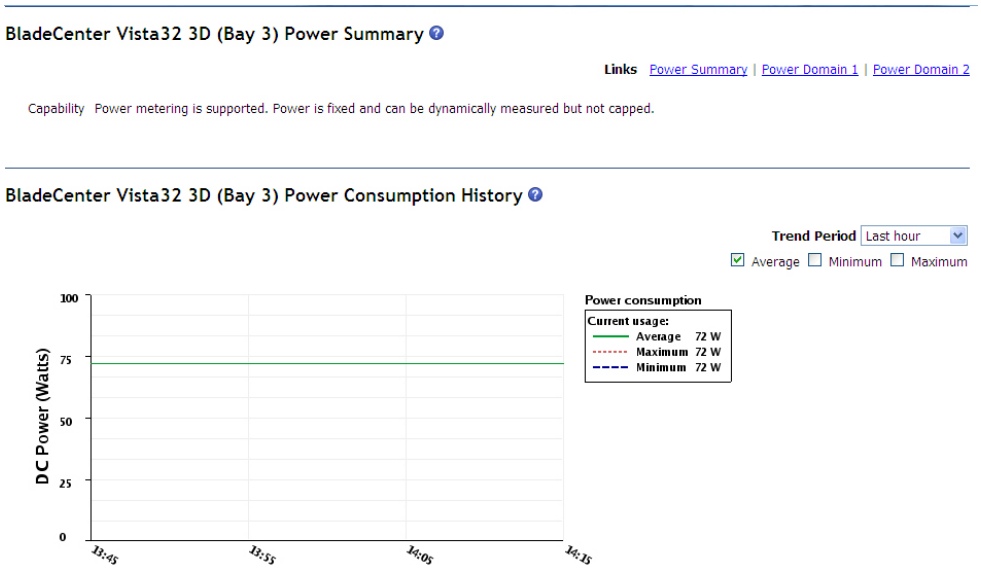
Power Domain 1 Totals

Total DC Power Available	3440W
Total Power in Use	210W
Maximum Allocated Power	272W

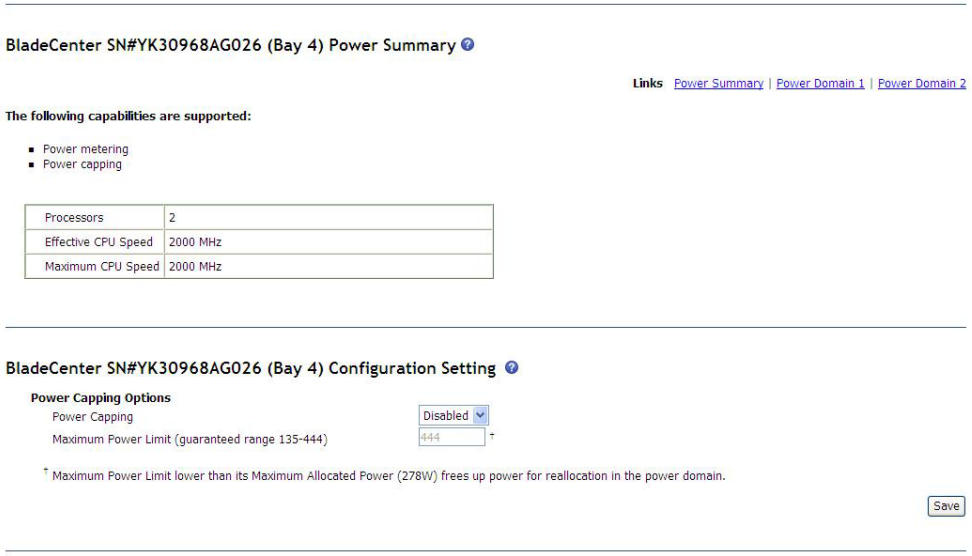
Refresh

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. Some BladeCenter components provide additional power information. The description of each component is a link that you can click to display a graph of additional detailed power information for the component. From the graph, you can select the types of power information that are shown: average power, maximum power, or minimum power. For blade servers, click the module name to display information about microprocessor performance.



For blade servers that have power configuration capability, the management module displays fields that you can use to enable or disable power capping and to set the maximum amount of power that the blade server can use. These fields are not shown for blade servers that do not support these advanced features.



The advanced management module displays information about allocated power and the power capping range for individual blade servers.

- The allocated maximum power is a typical maximum power for various configurations. It is used by the advanced management module to determine whether a blade server will fit within the power budget of the domain. If the power budget has sufficient reserves to support the blade server, the management module will power-on the blade server.
- The maximum power in the power capping range reflects the nameplate power for the blade server. This is not the same as the allocated maximum power.

You can set the maximum power capping value for an individual blade server. This value, specified in watts, is the power value to which a blade server is

capped by the advanced management module Power Management function. The maximum power capping value is persistent for all power cycles for blade servers.

Some server blades, including the JS12 and JS22, support soft power capping. When this feature is supported, the web page will display both the range and the guaranteed range.

– The **Range** is displayed as the soft capping minimum and capping maximum values.
– The **Guaranteed range** is displayed as the capping minimum and capping maximum values. Previous releases of the advanced management module firmware referred to this as the capping range.

Some server blades, including the JS12 and JS22, support Dynamic Power Saver, a power-saving mode that enables the blade server to selectively alter its operating voltage and frequency to reduce power consumption. See the blade server documentation for details. The following constraints apply to this feature.

– The **Dynamic Power Saver** setting is displayed only when the blade server is powered on.
– The **Guaranteed range** is displayed as the capping minimum and capping maximum values. Previous releases of the advanced management module firmware referred to this as the capping range.
– You can not enable **Static Low Power Saver** and **Dynamic Power Saver** at the same time.
– If the **Dynamic Power Saver** feature is not selected, the **Favor Performance over Power** check box is greyed out.

Some blade servers support Dynamic Power Saver

Note: The blade server must be powered-on for the power capping options to be available. If a blade server is removed from a BladeCenter unit or the BladeCenter unit is powered-off, the setting of the maximum power capping is lost.

Average power consumption on a blade server frequently does not reach or exceed the minimum power capping threshold. The minimum power capping threshold represents a value that can be guaranteed under all operating conditions. Total power consumption on a blade server is related to conditions that can include both the hardware configuration and the applications that are running on the blade server.

- **State**: This field displays the power state of the module (On or Standby).
- **Power in Use**: This field displays the amount of power, in watts, that is allocated to the module. Usually, a module consumes less power than the maximum allocated power. Therefore the total power that is actually consumed by the BladeCenter unit might be less than the amount that is shown in this field.
- **Maximum Allocated Power**: This field displays the maximum amount of power, in watts, that a component requires. The maximum allocated power for modules is the worst-case amount that the module can consume, but the power-in-use

number for some modules, such as I/O modules, the midplane, and the management module is the maximum allocated power when the module is powered-on. Usually, a module consumes less power than the maximum allocated power. Therefore, the total power actually consumed by the BladeCenter unit might be less than the amount that is shown in the **Power in Use** field.

- **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 support or report its duty cycles, `n/a` is displayed. A duty cycle is a ratio of actual processing time that is expressed as a percentage of total available processor time. For blade servers, click the module name to display information about microprocessor performance.
- **DOMAIN TOTALS**: These fields list the total power that is allocated for all components in the power domain.

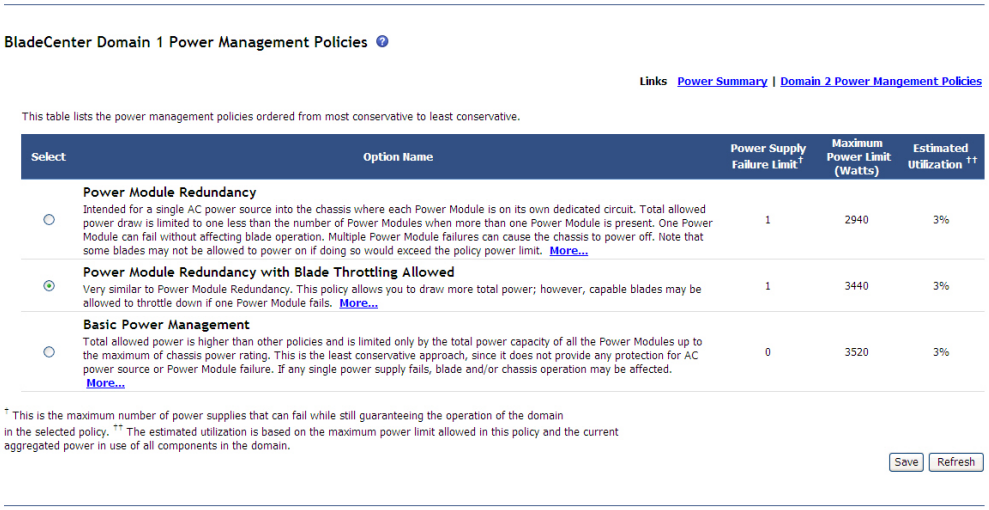
In this section, you can configure power management policy settings. The settings in this section apply to the entire BladeCenter unit, including the empty blade bays. You must have access to the BladeCenter unit and have either the Chassis Configuration role or Supervisor role to configure power-management policy settings. The settings are applied to each power domain independently. To ensure accurate reporting of power information, make sure that management-module firmware, blade server BIOS firmware, and Blade Systems Management Processor (BSMP) firmware are at the latest levels.

Blade server throttling achieves lower power consumption for a blade server by temporarily reducing the microprocessor performance. The advanced management module and the blade servers use power-management technologies that are built into certain microprocessors to throttle the blade servers to achieve lower power consumption.

Polices that enable throttling enable you to effectively use more total power from the BladeCenter unit, so that you can power-on more blade servers than would otherwise be possible. Blade servers might need to throttle to lower power consumption if a power module fails to keep the BladeCenter unit operational.

Note the distinction between ac power *sources* and power *circuits*. An ac power source is power that originates from a single power substation, such as a public power company, an on-site generator, or an uninterruptible power supply. A power circuit is power that comes from an ac power source and is limited by a circuit breaker. Having dual ac power sources means that you have power coming from more than one substation. Even though most server installations do not have this type of electrical setup, some of the policies are intended for use with dual power sources. You should have a dedicated circuit for each power module in your BladeCenter unit, regardless of the number of ac power sources that you have.

The name for the policy in effect for each power domain is a live link. Click a link to see a more detailed explanation of the policies, and to change the policy.



The following power management policies apply to the BladeCenter E, H, T, HT, and S units:

- **Basic Power Management** (default setting): This policy applies if the BladeCenter unit does not meet the recommended configurations for the other power policies. Blade servers power on, provided that the power that is consumed is less than or equal to the maximum total power limit for this policy. The total available power is higher for this than for other policies and is limited by the capacity of all power modules, up to a maximum of the BladeCenter unit power domain rating. The BladeCenter unit power domain rating might be lower than the total sum of all power module capacities. This is the least conservative policy for the BladeCenter unit power management.

  Note: If a power module fails, microprocessors on blade servers that are capable of throttling can throttle to reduce power consumption in the power domain. Power redundancy is not guaranteed and might result in the complete loss of power in the domain if the current power that is in use is higher than the capacity of the remaining power module.
- **Power-Module Redundancy**: This policy is intended for a single ac power source into the BladeCenter unit where each power module is on its own dedicated circuit. The maximum total power that is allocated within the power domain is limited to one less than the number of power modules when more than one power module is installed. One power module can fail without affecting blade server operation. Multiple power-module failures might cause all components within the power domain to power-off. Blade servers power-on only if they can operate unthrottled in case of power module failure. The number of blade servers that are able to power-on is determined by the maximum total power that is available from one less than the total number of power modules. If a single power module fails, all the blade servers that are powered-on will continue to operate at their unthrottled performance levels. If two or more power modules fail, the components within the power domain might power-off.
- **Power Module Redundancy with Blade Throttling Allowed**: This policy is intended for a single ac power source into the BladeCenter unit where each power module is on its own dedicated circuit. The maximum total power that is allocated within the power domain is limited to one less than the number of power modules when more than one power module is installed. Failure of one power module might cause blade servers to throttle, but the power domain would remain operational. Multiple power-module failures might cause all

components within the power domain to power off. This policy enables the components to draw more total power than the power module redundancy policy supports. With this policy, it might be possible to power on blade servers that a more restrictive policy would prevent. A possible side effect is that blade servers might need to throttle to lower power consumption in the case of one power-module failure to keep the power domain operational. Blade server throttling achieves lower power consumption for a blade server by temporarily reducing the microprocessor performance. The management module and the blade servers use power-management technologies that are built into certain microprocessors to throttle the blade servers to achieve lower power consumption. Not all blade servers are capable of throttling. Blade servers are able to power-on, provided that the power consumed is less than or equal to the maximum total power limit for this policy. If a single power module fails, processors on blade servers that are capable of throttling, might throttle to reduce the power that is consumed to less than or equal to the rated capacity of the power modules. Blade servers power-on in a throttled state in some configurations. When power redundancy is restored, the blade server microprocessors return to their unthrottled performance levels.

The BladeCenter S unit supports two additional power-management policy options:

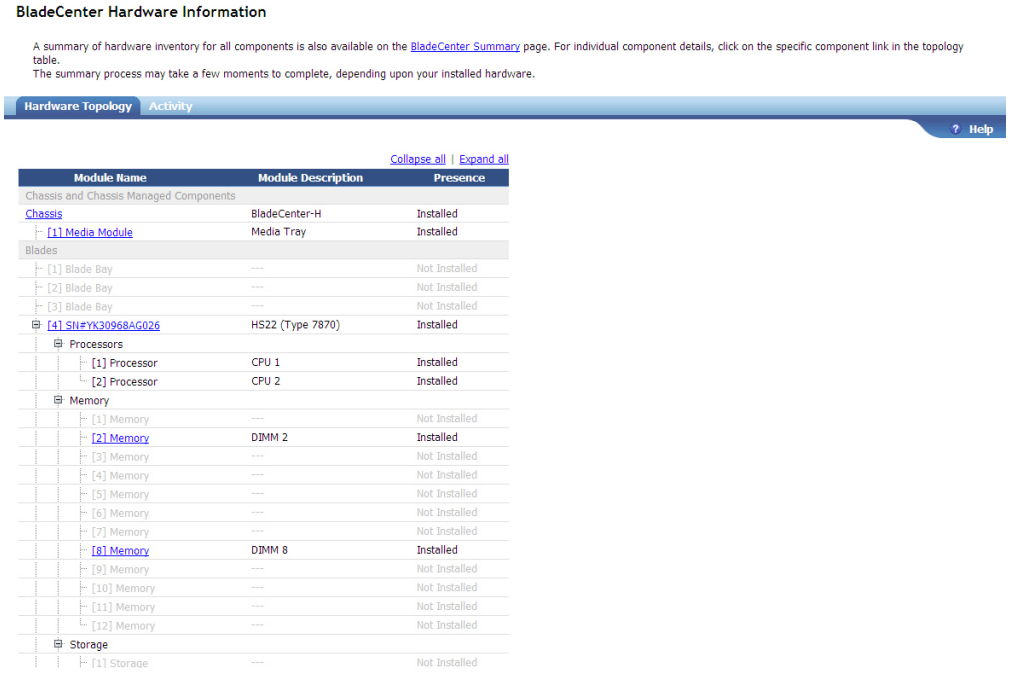
- **AC Power Source Redundancy**: This policy is intended for dual ac power sources into the BladeCenter unit. The maximum total power that is allocated within the power domain is limited to the maximum capacity of two power modules. This is the most conservative approach and is recommended when all four power modules are installed. When the BladeCenter unit is correctly wired with dual ac power sources, one ac power source can fail without affecting blade server operation. Note that some blade servers might not be able to power-on if doing so would exceed the maximum power limit of this policy.
- **AC Power Source Redundancy with Blade Throttling Allowed**: This policy is intended for dual ac power sources into the BladeCenter unit. The maximum total power that is allocated within the power domain is limited to the maximum capacity of two power modules. This is a conservative approach and is the best policy to use when all four power modules are installed. When the BladeCenter unit is correctly wired with dual ac power sources, failure of one ac power source might potentially cause some blade servers to throttle, but the BladeCenter unit remains operational. Note that some blade servers might not be able to power-on if doing so would exceed the maximum power limit for this policy. This policy enables components to draw more total power from the BladeCenter unit than the **AC power source redundancy** policy supports so that you can power-on blade servers that you might not otherwise be able to. A possible side effect is that in case of an ac power source failure, some blade servers might need to throttle to lower power consumption to keep the BladeCenter unit operational. Blade server throttling refers to achieving lower power consumption for a blade server by temporarily reducing the microprocessor throughput. The management module and the blade servers use power-management technologies that are built into certain processors to throttle the blade servers to achieve lower power consumption. Not all blade servers are capable of throttling.

Hardware VPD

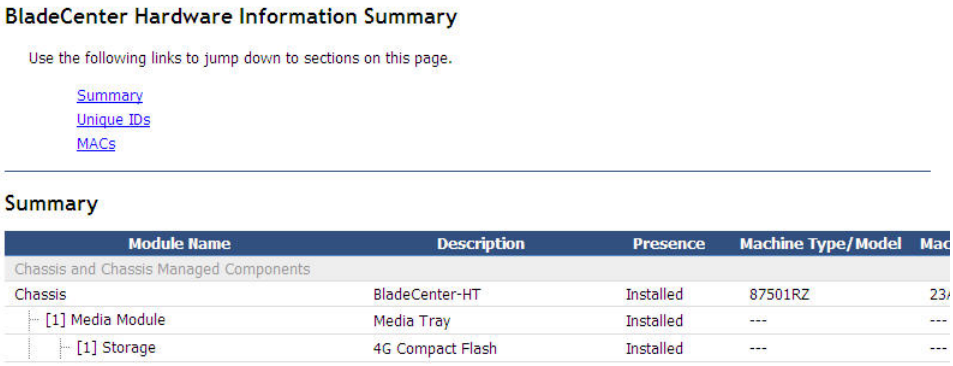
Select **Monitors → Hardware VPD** to view the hardware vital product data for the BladeCenter unit.

The following illustration shows the Hardware VPD page for an advanced management module. The page opens with the **Hardware Topology** tab displayed.

Note: This page also can display features that are unique to the BladeCenter S unit, including the Integrated Storage Modules, the Direct Serial Attach module, and the optional RAID SAS module.



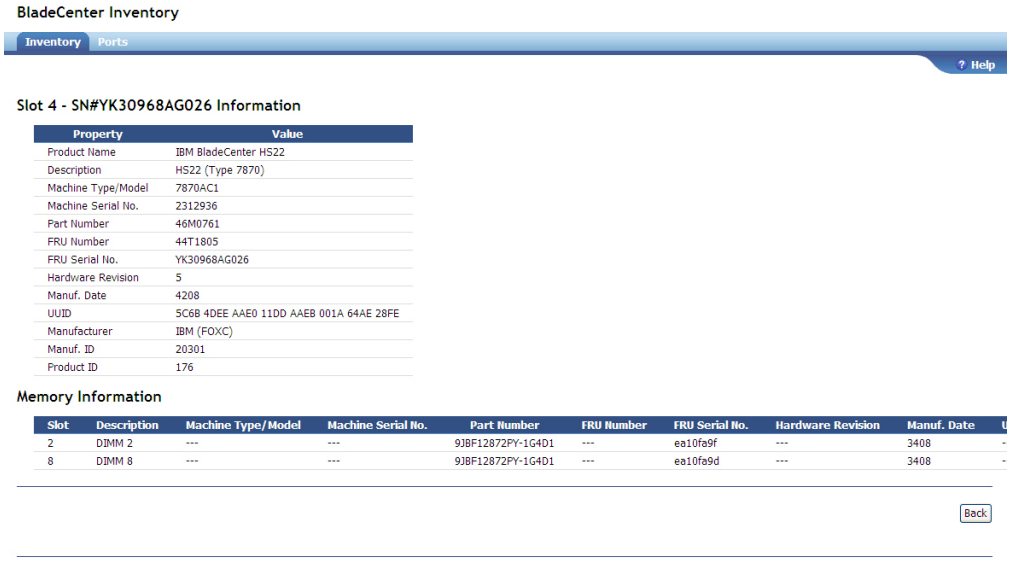
Select the BladeCenter Summary link to view a page that summarizes the hardware VPD.



Select **Monitors → Hardware VPD** to view the 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.



BladeCenter Inventory

Inventory | Ports

? Help

Slot 4 - SN#YK30968AG026 Information

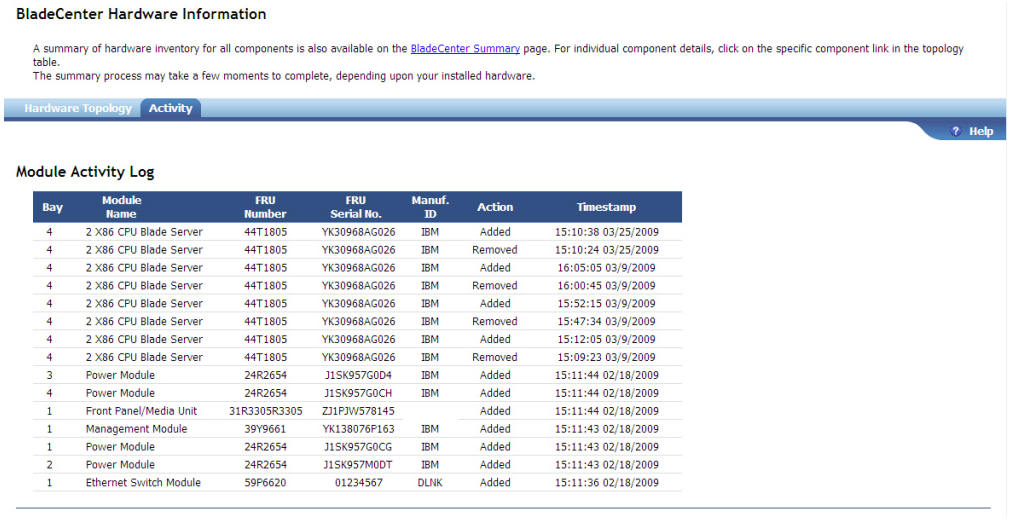
Property	Value
Product Name	IBM BladeCenter HS22
Description	HS22 (Type 7870)
Machine Type/Model	7870AC1
Machine Serial No.	2312936
Part Number	46M0761
FRU Number	44T1805
FRU Serial No.	YK30968AG026
Hardware Revision	5
Manuf. Date	4208
UUID	5C6B 4DEE AAE0 11DD AAEB 001A 64AE 28FE
Manufacturer	IBM (FOXC)
Manuf. ID	20301
Product ID	176

Memory Information

Slot	Description	Machine Type/Model	Machine Serial No.	Part Number	FRU Number	FRU Serial No.	Hardware Revision	Manuf. Date	U
2	DIMM 2	---	---	9JBF12872PY-1G4D1	---	ea10fa9f	---	3408	-
8	DIMM 8	---	---	9JBF12872PY-1G4D1	---	ea10fa9d	---	3408	-

Back

Click the **Activity** tab to view the log of modules that have been installed in or removed from the BladeCenter unit.



BladeCenter Hardware Information

A summary of hardware inventory for all components is also available on the BladeCenter Summary page. For individual component details, click on the specific component link in the topology table.
The summary process may take a few moments to complete, depending upon your installed hardware.

Hardware Topology | Activity

? Help

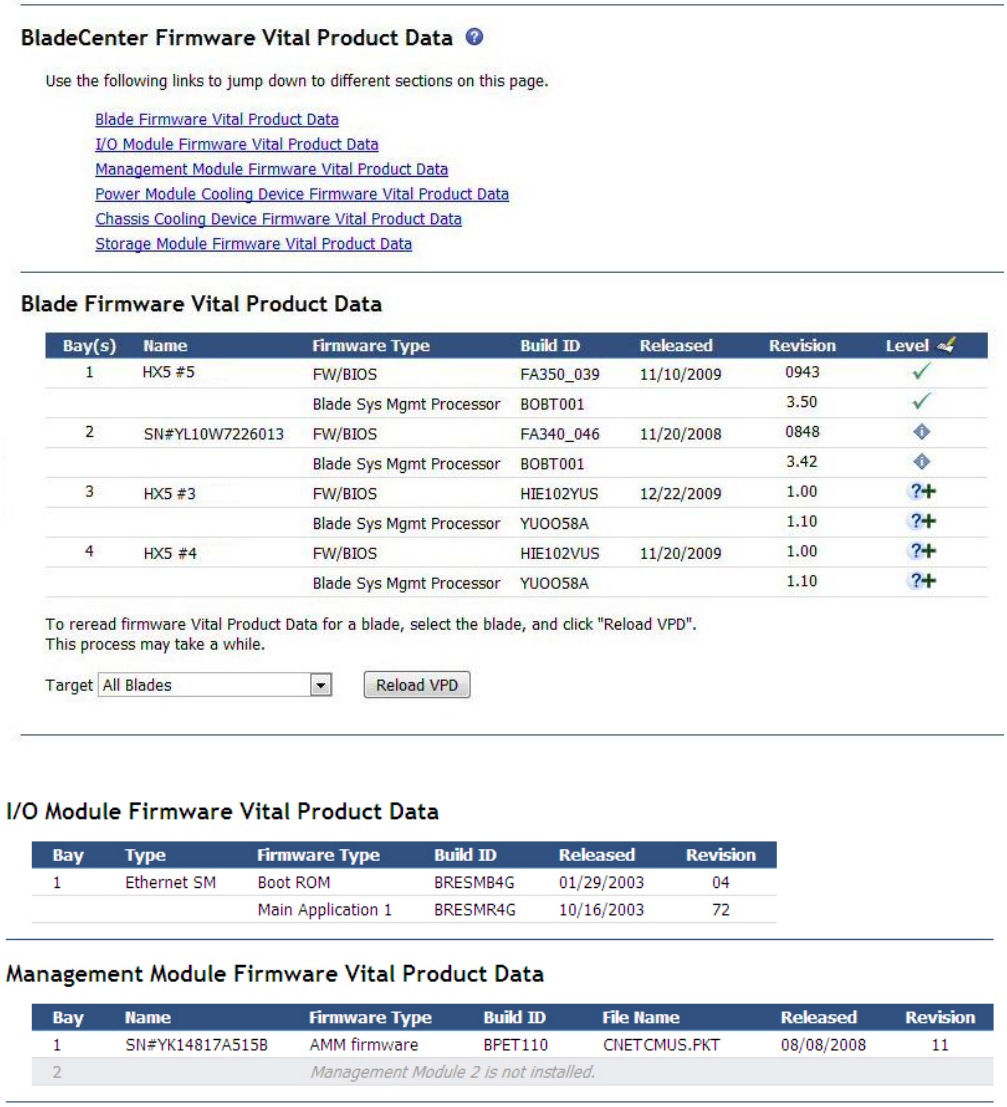
Module Activity Log

Bay	Module Name	FRU Number	FRU Serial No.	Manuf. ID	Action	Timestamp
4	2 X86 CPU Blade Server	44T1805	YK30968AG026	IBM	Added	15:10:38 03/25/2009
4	2 X86 CPU Blade Server	44T1805	YK30968AG026	IBM	Removed	15:10:24 03/25/2009
4	2 X86 CPU Blade Server	44T1805	YK30968AG026	IBM	Added	16:05:05 03/9/2009
4	2 X86 CPU Blade Server	44T1805	YK30968AG026	IBM	Removed	16:00:45 03/9/2009
4	2 X86 CPU Blade Server	44T1805	YK30968AG026	IBM	Added	15:52:15 03/9/2009
4	2 X86 CPU Blade Server	44T1805	YK30968AG026	IBM	Removed	15:47:34 03/9/2009
4	2 X86 CPU Blade Server	44T1805	YK30968AG026	IBM	Added	15:12:05 03/9/2009
4	2 X86 CPU Blade Server	44T1805	YK30968AG026	IBM	Removed	15:09:23 03/9/2009
3	Power Module	24R2654	J1SK957G0D4	IBM	Added	15:11:44 02/18/2009
4	Power Module	24R2654	J1SK957G0CH	IBM	Added	15:11:44 02/18/2009
1	Front Panel/Media Unit	31R3305R3305	ZJ1PJW578145		Added	15:11:44 02/18/2009
1	Management Module	39Y9661	YK138076P163	IBM	Added	15:11:43 02/18/2009
1	Power Module	24R2654	J1SK957G0CG	IBM	Added	15:11:43 02/18/2009
2	Power Module	24R2654	J1SK957M0DT	IBM	Added	15:11:43 02/18/2009
1	Ethernet Switch Module	59P6620	01234567	DLNK	Added	15:11:36 02/18/2009

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 page for an advanced management module.



BladeCenter Firmware Vital Product Data

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

Blade Firmware Vital Product Data
I/O Module Firmware Vital Product Data
Management Module Firmware Vital Product Data
Power Module Cooling Device Firmware Vital Product Data
Chassis Cooling Device Firmware Vital Product Data
Storage Module Firmware Vital Product Data

Blade Firmware Vital Product Data

Bay(s)	Name	Firmware Type	Build ID	Released	Revision	Level
1	HX5 #5	FW/BIOS	FA350_039	11/10/2009	0943	✓
		Blade Sys Mgmt Processor	BOBT001		3.50	✓
2	SN#YL10W7226013	FW/BIOS	FA340_046	11/20/2008	0848	◆
		Blade Sys Mgmt Processor	BOBT001		3.42	◆
3	HX5 #3	FW/BIOS	HIE102YUS	12/22/2009	1.00	?+
		Blade Sys Mgmt Processor	YUOO58A		1.10	?+
4	HX5 #4	FW/BIOS	HIE102VUS	11/20/2009	1.00	?+
		Blade Sys Mgmt Processor	YUOO58A		1.10	?+

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

Target All Blades Reload VPD

I/O Module Firmware Vital Product Data

Bay	Type	Firmware Type	Build ID	Released	Revision
1	Ethernet SM	Boot ROM	BRESMB4G	01/29/2003	04
		Main Application 1	BRESMR4G	10/16/2003	72

Management Module Firmware Vital Product Data

Bay	Name	Firmware Type	Build ID	File Name	Released	Revision
1	SN#YK14817A515B	AMM firmware	BPET110	CNETCMUS.PKT	08/08/2008	11
2		*Management Module 2 is not installed.*				

Note: The management module needs to be restarted before it can use a newly downloaded firmware image. This page will display, on separate lines, vital product data about both the current and the pending software loads.

Click **Firmware Vital Product Data** to view the 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.

- When an advanced management module is installed in some BladeCenter units, you also can view the VPD for the chassis cooling unit and power-supply cooling unit firmware.

Power Module Cooling Device Firmware Vital Product Data

Bay	Firmware Type	Revision
1	Fan controller	14
2	Fan controller	14
3	Fan controller	14
4	Fan controller	14

Chassis Cooling Device Firmware Vital Product Data

Bay	Firmware Type	Revision
1	Fan controller	14
2	Fan controller	14

- For an advanced management module that is installed in a BladeCenter S unit, you also can view the VPD for the storage-module firmware.

Storage Module Firmware Vital Product Data

Bay	Firmware Type	Build ID	Released	Revision
1	Storage Module	S4SM06X65.DS1	10/09/2007	X.65
2	Storage Module	S4SM06070.DS1	10/25/2007	0.70

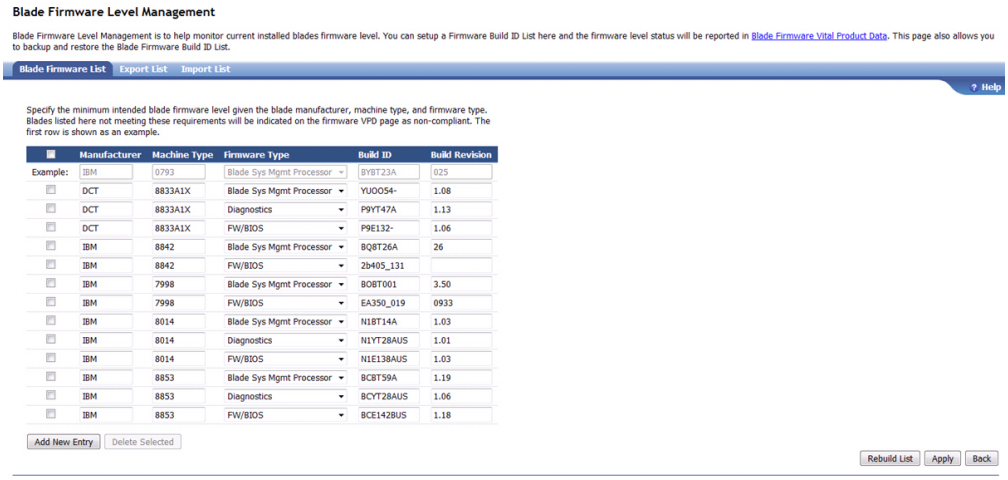
The firmware VPD includes the firmware type and version information such as a build ID, release date, and revision number. The VPD information varies by BladeCenter component type; for example, the VPD for the management-module firmware might also include the file name of the firmware components. (After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

For blade servers, the level status compares the firmware build level for all blade servers in a BladeCenter unit and the build levels in the optional Blade Firmware List, providing one of the following indications:

- If the level status indication for a blade server is blank, the firmware for the blade server is not being checked.
- The  icon indicates that like blade servers have the same firmware level or that firmware on the blade server matches the requirements specified in the Blade Firmware List. Click on the icon to view and edit the Blade Firmware List.
- The  icon indicates that like blade servers have different (mismatched) firmware levels or that the firmware on the blade server does not match the requirements specified in the Blade Firmware List. Click on the icon to update the blade server firmware.
- The  icon indicates a unique blade server (there is only one blade server of a type installed in the BladeCenter unit) and that no firmware requirements are specified for this blade server type in the Blade Firmware List. Click on the icon to edit the Blade Firmware List, where a new entry will automatically be created for the blade server type. After firmware information is entered for the blade server, the configuration needs to be saved for the changes to take effect.

Click the  icon at the top of the Level column to view, edit, download, or upload build ID levels in the Blade Firmware List.

The list of blade server firmware VPD is initially generated based on what is detected in the BladeCenter unit and displays in the Blade Firmware List on the Blade Firmware Management page.



In the Blade Firmware Management page, blade server firmware VPD information can be edited in the Blade Firmware List tab. Clicking **Rebuild List** will scan the BladeCenter unit and generate a list of blade server firmware VPD based on what is detected. The list contains information for only those blade servers that have VPD which is fully accessible by the advanced management module. Any blade servers with VPD that is unavailable or failed will be ignored and not appear in the list. This list can then be modified manually to specify different requirements. You must make sure to enter information in the manufacturer, machine type, firmware type, and build ID fields.

The Export List and Import List tabs allow the blade server firmware VPD, as seen on the Blade Firmware List tab, to be saved to or loaded from a file. The blade server firmware VPD file filename is automatically named in the form *ammName*_*YYYYMMDD*_*hhmmss*_buildids, where:

- The *ammName* indicates the name of the advanced management module
- The *YYYYMMDD* indicates the date of blade server firmware VPD export in year-month-day format.
- The *hhmmss* indicates the time of blade server firmware VPD export in hour-minute-second 24-hour clock format.

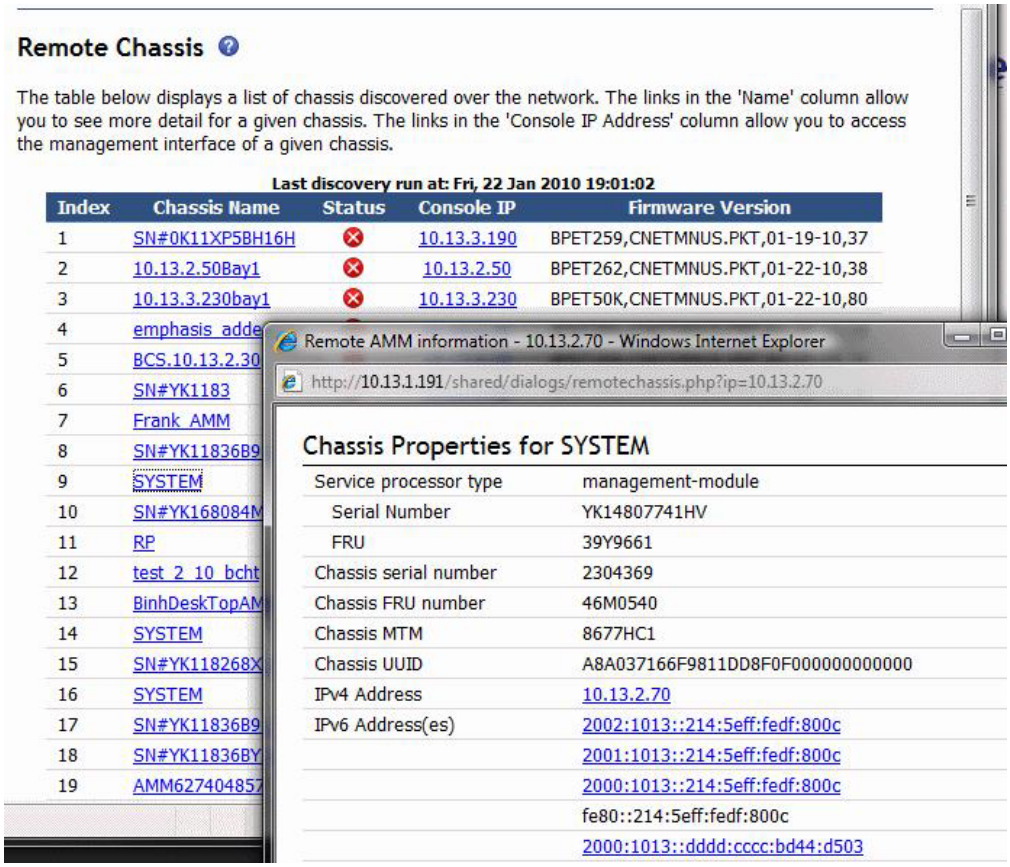
When an optional standby advanced management module is installed, the active advanced management module mirrors data and firmware updates to it. The firmware VPD for both the active and standby advanced management modules are displayed on this page. If the active advanced management module detects that the standby advanced management module is at a different firmware level, it attempts to update the standby advanced management module to the same level. Unless this operation is in progress, the firmware VPD should be identical for the active and standby advanced management modules.

Note: The BladeCenter S unit has one advanced management module and does not support an optional standby advanced management module.

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

Remote Chassis

Select **Monitors → Remote Chassis** to view a list of all BladeCenter units that are found on the network.



The **Remote Chassis** page uses the Service Location Protocol (SLP) to find and display information for all BladeCenter units on the network. This information includes the BladeCenter unit name, status, management-module IP address, and management-module firmware version. Click the BladeCenter unit name to display a detailed view of the properties of that BladeCenter unit. Click the console IP address of the BladeCenter unit to start a web interface session for that BladeCenter unit. SLP must be enabled in the “Network Protocols” on page 170 page for the Remote Chassis list to be populated.

Click **Discover** to force an immediate network search to repopulate the remote BladeCenter unit list.

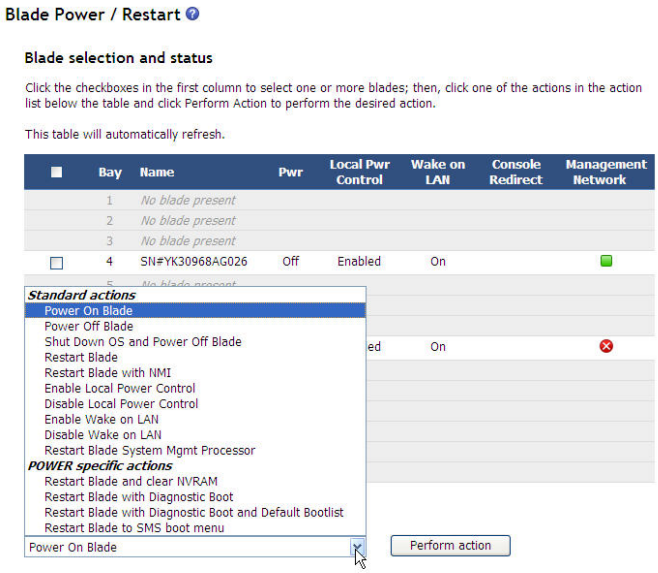
Click **Clear** to clear the remote BladeCenter unit list. The list is not repopulated until you click **Discover**.

Blade Tasks

Select the **Blade Tasks** choices to view and change the settings or configurations of the 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.



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).

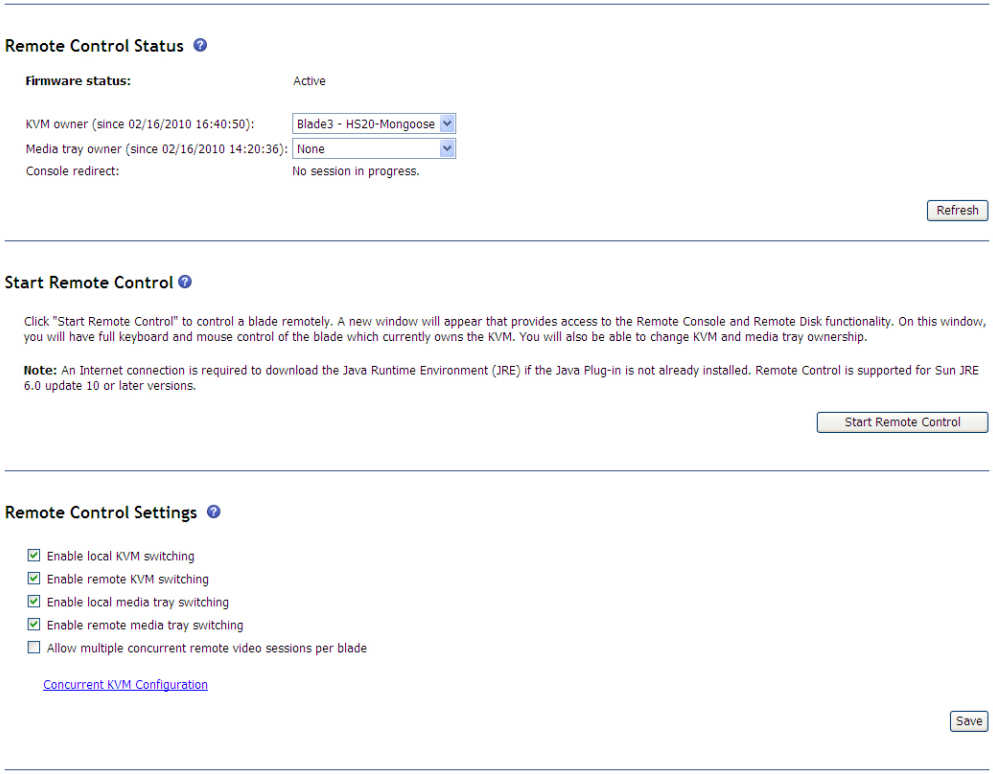
The following operations can be performed on some POWER-based blade servers.

- Restart the selected blade server and enter the System Management Services (SMS) menu.
- 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 assign local KVM or Media Tray to specific blade servers, or to operate a blade server from a networked remote console.

The following illustration shows the remote-control page for an advanced management module.



To assign the local KVM or the media tray to a different blade server, select the blade server from the **KVM owner** list or **Media tray owner** list and click **Refresh**.

Click **Start Remote Control** to establish a remote console. The remote console launches in a stand-alone Java application window (see "Using the remote console feature" on page 69 for more information).

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+S to the blade server, click the **Ctrl** icon, click inside the video area, then press the **S** key on the keyboard.

Use the remote console to perform the following tasks:

- View and change the blade server that currently controls the Keyboard, Video, and Mouse (KVM) and the media tray in the BladeCenter unit. See the *Installation and User's Guide* for your blade server for more information about KVM and media tray switching.

Notes:

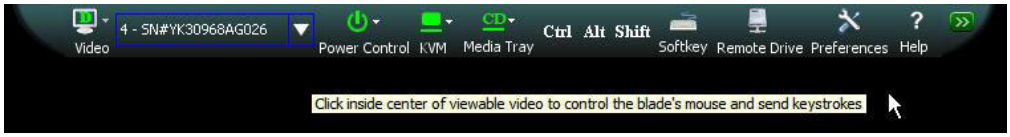
- The operating system in the blade server must provide USB support for the blade server to recognize and use the keyboard and mouse, even if the keyboard and mouse have PS/2-style connectors.
- If the operating system in the blade server does not support USB Mass Storage, the remote disk feature is 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 70 for information and instructions.
- 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 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 features are supported:

- Enable or disable remote switching of the media tray for all blade servers until they are explicitly enabled again.
- Enable or disable remote KVM switching for all blade servers until this feature is explicitly enabled again.
- Enable or disable multiple concurrent video sessions. If the sessions are enabled, up to four users can view the video of the same blade server concurrently through the remote console; otherwise, the video can be viewed by only one user.

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



For the advanced management module, the remote console video controls are consolidated into a taskbar at the top of the screen.

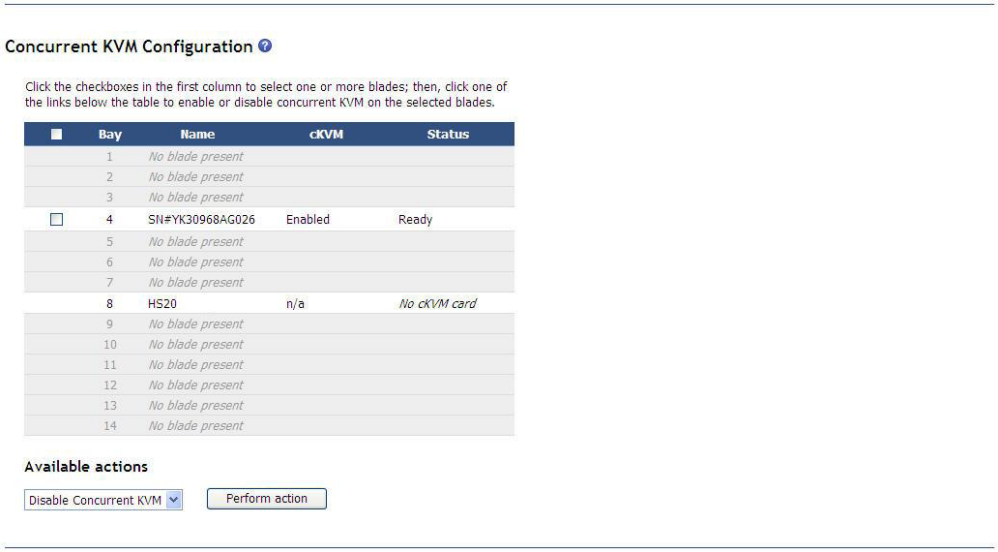
- Use the **Video** icon to repaint, calibrate, or adjust the horizontal position of the display.
  - Select **Toggle Full Screen** to switch between display of the remote session in a sizable window and a view that takes up the entire screen. This feature is available only when viewing a concurrent video blade server.
  - Select **Repaint** to update the remote console display and clean up display artifacts.
  - Select **Calibrate** (does not apply to cKVM blade server sessions) to run a video calibration sequence that optimizes remote video session performance. Calibrate a session when the displayed colors are significantly different from what is expected.
  - Select **Horizontal Adjust** to center the display.
  - Select **Screenshot** to capture the current video screen and save it to the local disk drive in one of the supported image formats. This feature is available only when viewing a concurrent video blade server.

  Note: These operations do not apply to cKVM video.
- Use the **Server Blade** dropdown list to select the blade server to control.
- Use the **Power Control** icon to power-off the selected blade server, to restart it, to stop the operating system and power-off, or to restart it with an NMI.
- Use the **KVM** icon to assign the local KVM to a selected blade server.
- Use the **Media tray** icon to assign the Media tray to a selected blade server.
- Use the **Sticky Key** buttons to modify your next keystroke with the Ctrl, Alt, or Shift key.
- Use the **Softkey** icon to define or use custom keystroke sequences.
- Use the **Remote Drive** icon to open the Remote Drive window, which is used to mount and unmount virtual media. See “Mounting a disk drive or image” on page 70.
- Use the **Preferences** icon to set remote-control session preferences, to set KVM preferences, and to create custom key icons that represent common key combinations. You can also disable or enable the mouse capture feature that allows the local computer mouse to control either the remote session or the local computer, based on its screen position. When mouse capture is disabled, you also have the option of enabling or disabling the local mouse.

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.

Click **Concurrent KVM Configuration** to view and configure the concurrent KVM (cKVM) status and settings for each blade server. The concurrent KVM feature

requires optional hardware and a blade server that is concurrent KVM capable. See the documentation for your blade server for additional information.



When concurrent KVM is used, multiple remote-control sessions can access multiple blade servers simultaneously. Standard remote-console sessions (not using concurrent KVM) enable only one remote-console session for one blade server at a time. If multiple concurrent remote video sessions are enabled in the Remote Control Settings, up to four users can view the video of the same blade server concurrently through the remote console; otherwise, the video can be viewed by only one user. If the maximum number of active remote-control sessions has been reached, you must end one of the current sessions to start a new one.

Firmware Update

Select **Blade Tasks → Firmware Update** to update some types of firmware on a blade server.

Important:

- Some cluster solutions require specific code levels or coordinated code updates. If the device is part of a cluster solution, verify that the latest level of code is supported for the cluster solution before you update the code.
- All blade servers in a scalable complex must be at the same firmware level. See “Firmware Multi-flash” on page 128 for information about performing a coordinated update of firmware for multiple blade servers.

Use this page to update the firmware on a specific blade server. Currently, the blade server Blade System Management Processor (BSMP) or service processor firmware can be updated on most blade server types by using this page. Blade server BIOS or Unified Extensible Firmware Interface (UEFI) update is also supported by this page for some blade server types. This page does not support the update of blade server BIOS for most blade servers, or the update of diagnostics, network adapter or cKVM adapter firmware. See the documentation that comes with your firmware update for detailed information and instructions about updating firmware.

Select the target blade server and the firmware file to use for the update; then, click **Update**. If more than one blade server is installed in the BladeCenter unit that supports multi-flash firmware update, multiple blades of the same type can be selected (see "Firmware Multi-flash" on page 128 for additional information). If scalable complexes are enabled for your BladeCenter unit (the default setting), all blade servers that are in the complex with the blade server that you selected will be selected automatically. Deselecting any blade servers in the scalable complex will cause all of the blade servers in that complex to deselect. If scalable complexes are disabled for your BladeCenter unit, you can select and deselect the check boxes for multiple multi-flash capable blade servers of the same type to perform a simultaneous firmware update.

You can obtain the firmware files from http://www.ibm.com/systems/support/.

The Remote File method enables you to specify the fully qualified address of the firmware packet file for updating the BSMP firmware. The fully qualified address contains a protocol that is supported by the advanced management module followed by a colon and two forward slashes (//), the username and password separated by a colon for login authentication, an @ sign followed by the hostname or IP address, an optional port number, and the full path file name.

Note: If the port number is specified, it must be separated from the hostname (or IP address) by a colon.

The complete format is: *protocol*://*username*:*password*@*hostname*:*port*/*path*/*filename*

The advanced management module supports the following protocols:

- tftp
- ftp
- ftps
- http
- https

An example of a fully qualified address is:

```
ftp://USERID:PASSW0RD@192.168.0.2:30045/tmp/CNETCMUS.pkt
```

In this example, the ftp protocol will be used for transferring the packet file, the username is `USERID`, password is `PASSW0RD`, host IP address (IPv4) is `192.168.0.2`, port number is `30045`, and `/tmp` is the full pathname to the packet file `CNETCMUS.pkt`.

Some protocols do not need the username, password, and the port number, so the minimum requirement for a fully qualified address can be:

protocol://hostname/path/filename

To update advanced management module firmware by using a remote file, complete the following steps:

1. Check the **Remote File** checkbox.
2. Type in a fully qualified address in the textbox.
3. Click either the **Update** or **Update and Reboot** push button.

Note: If you are using a hostname instead of an IP address to specify a remote file, make sure DNS is enabled.

Firmware Multi-flash:

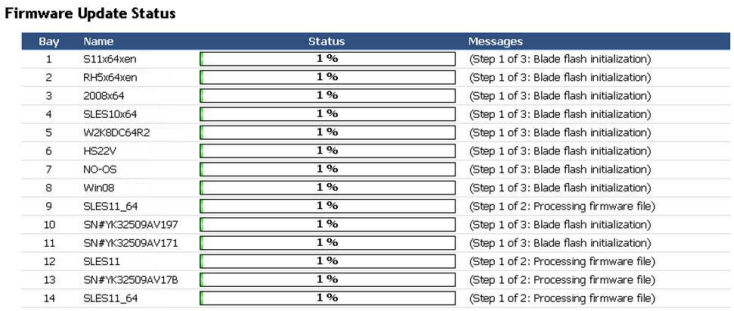
For a specific firmware level and blade server type, the advanced management module allows you to select multiple blade servers and update their firmware simultaneously.

Note:

- The firmware multi-flash feature and the Firmware Update Status page are available only when blade servers that support this feature are installed in the BladeCenter unit.
- If a blade server has more than one type of firmware that needs to be updated, each update must be performed separately.

After blade servers are selected for multi-flash update, you select the firmware file to be updated on the selected blade servers. Each blade server is then updated as a separate process.

The following illustration shows the multi-flash status page for coordinated blade server firmware updates.



Note: During multi-flash updates, the advanced management module does not check that a blade server is available for update before attempting to update its firmware. Blade servers that are not in a state that is ready for update will fail the update.

The Firmware Update Status page shows the progress for each blade server being updated. If any blade server fails an update operation, the advanced management module will generate an event log entry describing the problem: you should not

make another attempt to update the firmware until you review these entries. If the selected firmware file is not compatible with all or some of the blade servers selected, the failures will be indicated as a separate event for each blade server that fails.

Configuration

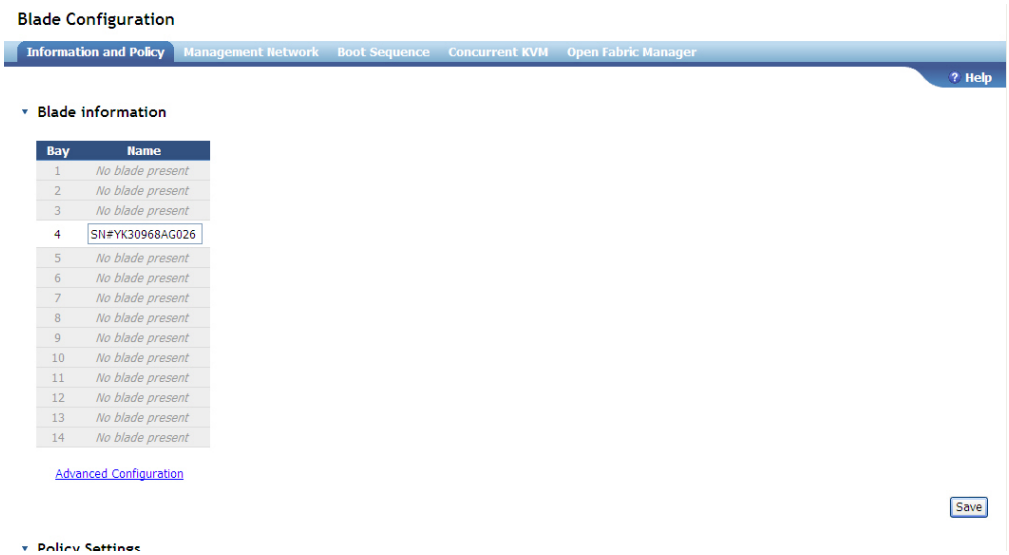
Select **Blade Tasks → Configuration** to view and change blade server configuration settings.

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

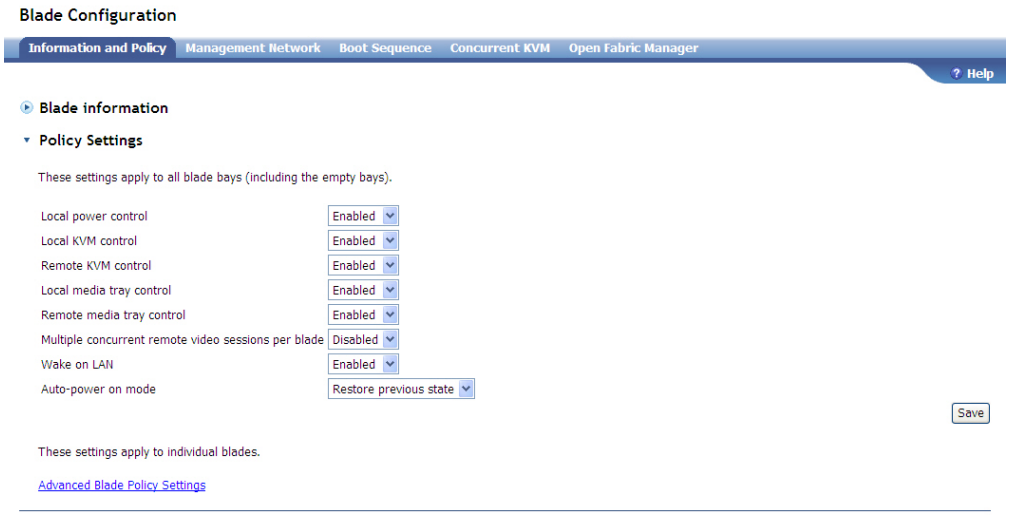
Note: Open Fabric Manager is not a standard advanced management module feature but is sold and documented separately. See the *BladeCenter Open Fabric Manager* documentation for more detailed information. See "License Manager" on page 181 for information about how to purchase the Open Fabric Manager feature.

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

- View the bay locations and names of the installed blade servers
- Access the "Advanced Configuration" on page 134 page to view or edit blade bay data



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

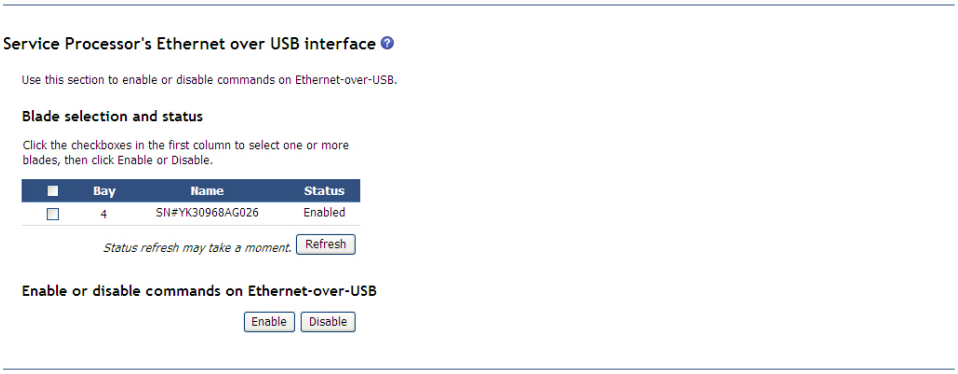


- **Local power, KVM, and media tray control**: These fields display the global policy setting for all blade bays. When set to **Enabled**, the feature is enabled for all bays. When set to **Disabled**, the feature is disabled for all bays. The value of **Not set** indicates that no global policy has been set; some bays might have the feature enabled while other bays have it disabled.
- **Remote KVM and media tray control**: This field displays the global policy setting for all blade bays. When set to **Enabled**, the feature is enabled for all bays on the Remote Control applet. When set to **Disabled**, the feature is disabled for all bays on the Remote Control applet. 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). If the remote disk or remote KVM feature is disabled, its field will be disabled. You can enable the remote disk by going to the **MM Control → Network Protocols → Remote Control** page.
- **Multiple concurrent remote video sessions per blade**: This field displays the global policy setting for whether multiple concurrent remote video sessions are supported on each blade server. When set to **Enabled**, a maximum of four users can concurrently view the video of the same blade server using the remote console applet. When set to **Disabled**, only one remote video session will be supported at a time on each blade server. The value of **Not set** indicates that this global policy has not been initialized and only one remote video session will be supported at a time per blade server.
- **Wake on LAN**: This field displays the global policy setting for the Wake on LAN function 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 other bays 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.
- **Auto-power on mode**: This field displays the global automatic power-on policy setting for all blade bays. When set to **Auto power**, all blade servers automatically power on, subject to power permission, when power is applied to the BladeCenter unit, regardless of their previous power state. When set to **Manual power**, all blade servers are left off, when power is applied to the BladeCenter unit, until manually powered on by the user. When set to **Restore previous state** (the default setting), the advanced management module attempts to power on all blade servers, when power is applied to the BladeCenter unit, that were previously powered on.

Note:

- If the BladeCenter unit hardware configuration changed since the last known power state, no blade servers will be powered on.
- A restart of the BladeCenter unit is required before any changes to the automatic power-on policy settings will take effect.

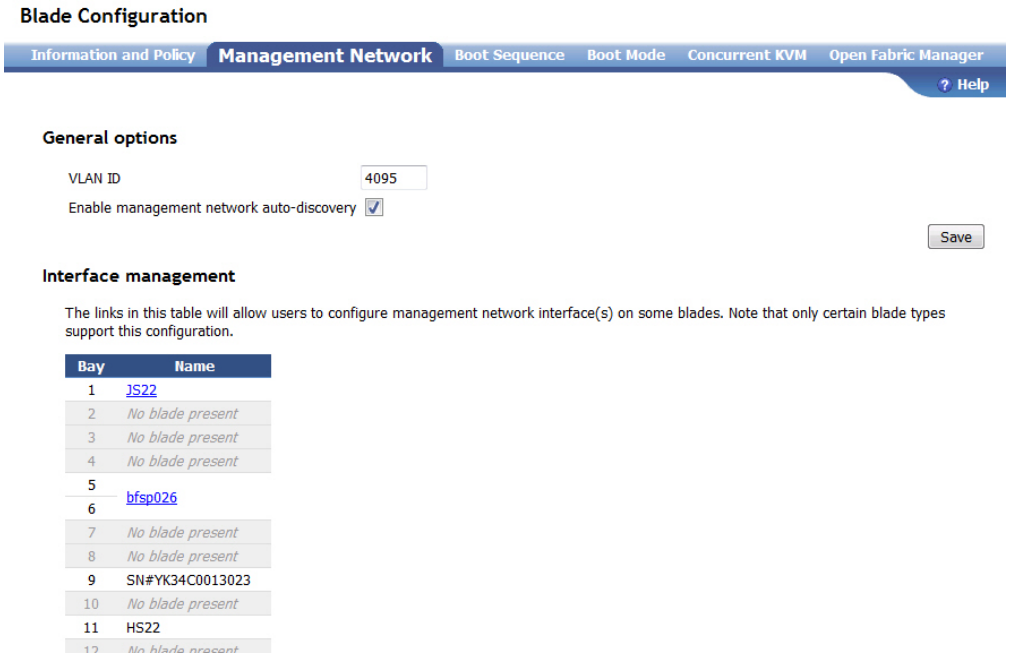
- Click **Advanced Blade Policy Settings** to access the page where you disable or enable the Ethernet interface on each blade server service processor. When installing some Linux operating systems over a network, some service processors need to have their Ethernet over USB interface disabled. Advanced blade policy settings are not supported by all blade servers.



Click **Management Network Configuration** to configure the VLAN ID for the internal management network that is used to communicate between the advanced management module and the blade server BSMPs. Selecting **Enable management network auto discovery** allows each management channel auto discovery (MCAD) capable blade server and the advanced management module to determine which communication channel to use based on the expansion cards that are installed on a blade server and the I/O modules that are installed in the BladeCenter unit. The communication path is automatically given higher priority for high-speed I/O Modules. Management channel auto discovery operation is controlled by the BSMP or an MCAD-capable service processor. A user can not manually specify the management communication path. See “Using management channel auto-discovery” on page 72, the *BladeCenter SOL Setup Guide*, and the documentation for your blade server for additional information about configuring MCAD.

For each blade server that supports manual configuration of its management network interface, a link is provided in the Interface Management section. Clicking this link displays a screen where you can set up the network configuration for the service processor on the blade server. See “Configuring a blade server management network” on page 20 and the documentation for your blade server for additional information about manually configuring a blade server management network.

Note: This feature is not supported by all blade servers.



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.

The following boot sequences for your BladeCenter unit and blade servers are available. Additional boot devices might be available for some blade server types.

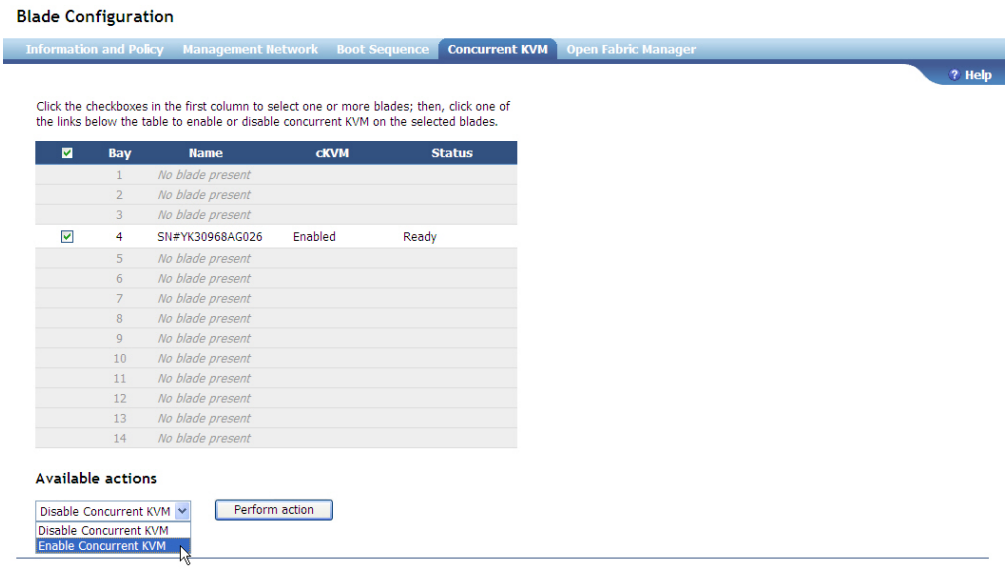
- **Hard disk drives** (0 through 4). The selection of hard disk drives depends on the hard disk drives that are installed in your blade server.
- **CD-ROM** (optical drive).
- **Diskette drive** (some BladeCenter unit types)
- **Network - PXE**. Selecting Network - PXE attempts a PXE/DHCP network startup the next time the blade server is turned on or restarted.
- **USB modular flash drive**

  Notes: The advanced management module has two USB ports. If you connect a USB storage device to one USB port, blade servers in the BladeCenter unit also can use it. The rules that determine which blade server detects the USB storage device are as follows:
  - For the BladeCenter unit, the USB storage device mounts to the blade server that has ownership of the KVM.
  - For the BladeCenter H or HT unit, the USB storage device mounts to the blade server that has ownership of the media tray.
  - The advanced management module for the BladeCenter T unit does not have external USB ports.
  - To use the optical drive or diskette drive (some BladeCenter unit types) as a boot-record source for a blade server, the blade server must have been designated as the owner of the optical drive, diskette drive (if it is supported for your BladeCenter unit), and USB port. You set ownership either by pressing the CD/diskette/USB select button on the blade server or through the **Remote Control** choice, described in "Remote Control" on page 123.
  - Some blade servers do not support the option of booting from a diskette drive.
- iSCSI boot devices. Select **iSCSI Critical** to force the blade server to search for an iSCSI boot device until it finds one.

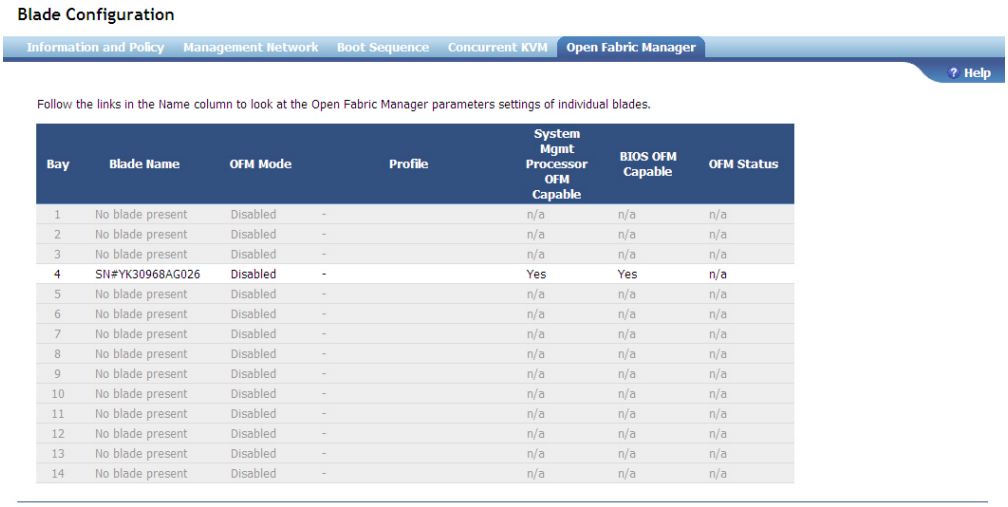
Click **Boot Mode** to select which BIOS or system firmware copy to use when you boot the blade server. You can select a primary (temporary) copy or a secondary (permanent) copy. You should boot from the temporary copy because it typically contains the latest enhancements and updates. Switching to the permanent copy should be reserved for cases when booting from the temporary copy is no longer possible. Changes to the boot mode setting take effect after the next restart of the blade server.

Note: This feature is not supported by all blade servers.

Click **Concurrent KVM Configuration** to display a list of bays, blade servers, and their cKVM status. Click the check boxes in the first column to select one or more blade servers; then, click one of the links below the table to enable or disable concurrent KVM on the selected blade servers.

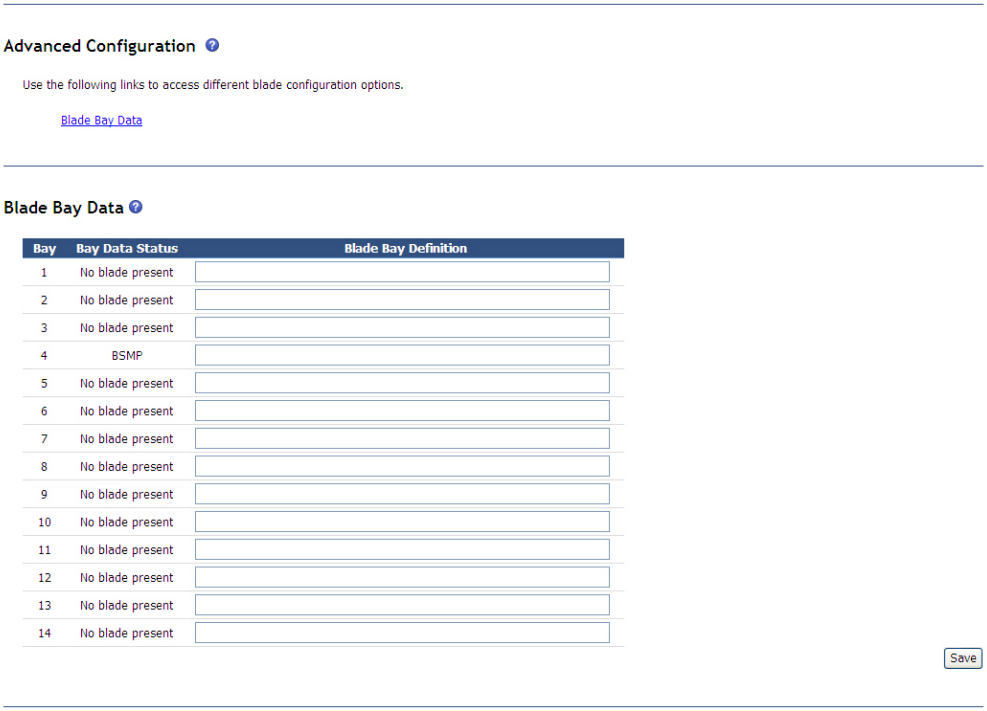


If your BladeCenter unit uses the optional Open Fabric Manager feature, click **Open Fabric Manager Parameters** to display a list of bays, blade servers, and their Open Fabric Manager parameters; then, click one of the links to view the detailed information for individual blade servers.



Advanced Configuration:

Select **Blade Tasks → Configuration → Advanced Configuration** to view and edit blade bay data.



Click **Advanced Configuration** in the Blade Information page to view and edit blade bay data.

Blade bay data is stored on the advanced management module nonvolatile RAM (NVRAM) and is associated with the BladeCenter unit blade bay. If you move a blade server to a new or different bay, the blade server gets the blade bay data of new bay; any previous blade bay data in the blade server is overwritten.

Blade bay data enables the blade server operating system to read bay-specific data on initialization to help configure itself. This data can specify information such as which device drivers or software options to load, whether the blade server is a master or member in a high availability system, the chassis number, the IP address, and the code load to use for the Preboot Execution Environment (PXE).

You can enter up to 60 alphanumeric characters into the **Blade Bay Definition** field to define blade bay data. Click **Save** when you have finished configuring one or more blade bay data definitions. It might take the advanced management module several minutes to update these fields.

The blade server operating system can read blade bay data either directly from the blade server BSMP or through the blade server BIOS SMBIOS (System Management BIOS) structure. The blade server operating system can use either or both methods. There are advantages and disadvantages to both:

- Blade bay data is available from the BSMP immediately after it is saved in the management module; however, more device drivers and code must be operational on the blade server for it to issue IPMI commands to the BSMP.
- The operating system can access SMBIOS data sooner during initialization with less operational code; however, the BIOS must be run again whenever blade bay data is defined or changed in the management module. You must power-off and power-on, restart, or remove and reinstall the blade server to put the latest blade bay data into the BIOS SMBIOS data structure.

The **Bay Data Status** column indicates the current support and status of the blade server. The following status values are defined:

Blade not present
No blade server is installed in bay.

Unsupported
The blade server BSMP firmware does not support blade bay data functions. You might be able to upgrade the BSMP firmware to a version that supports blade bay data.

BSMP
The blade server BSMP supports blade bay data, but BIOS has not read the current blade bay data definition. This is an operational state. The blade server operating system can read blade bay data from the BSMP. If the blade server BIOS has not read blade bay data, it must be restarted, or the BIOS firmware level must be updated to a level that will support blade bay data.

Supported
The blade server fully supports blade bay data. The latest blade bay data definition is in both the BSMP and the BIOS SMBIOS structure.

Discovering
The advanced management module is discovering a blade server.

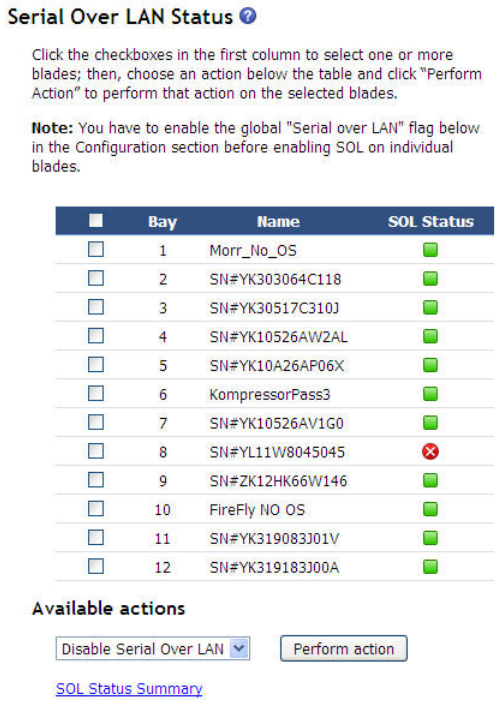
Note: You can define blade bay data even if the blade server does not support blade bay data or is not installed.

Blade bay data write operations require Blade Configuration authority. If you do not have authority to change these fields, the fields are not available.

See the *BladeCenter Management Module Command-Line Interface Reference Guide* for information and instructions for using the management-module command-line interface to perform these tasks.

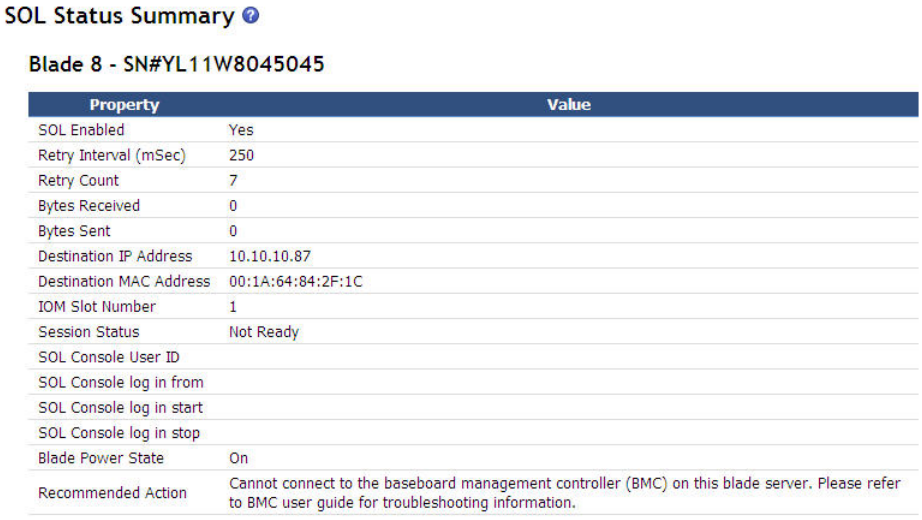
Serial Over LAN

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



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.

Click the **SOL Status** icon for a blade server to see a detailed summary of that blade server's condition, and recommended actions.



Click the **SOL Status Summary** link to see the status summary information for all the blader servers managed by the advanced management module.

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

Note: For the advanced management module, the **VLAN ID** used by SOL is set on the **Blade Tasks → Configuration** page. This page also allows you to enable management channel auto discovery, that allows SOL to communicate through any of the I/O modules installed in the BladeCenter unit. See “Configuration” on page 129 for information.

Start and run SOL sessions by using the management-module command-line interface. See the *BladeCenter Advanced Management Module Command-Line Interface Reference Guide* and the *Serial over LAN Setup Guide* for further information.

Open Fabric Manager

Select **Blade Tasks → Open Fabric Manager** to manage interfaces and hardware adapters.

This task is in the navigation panel under **Blade Tasks** for advanced management modules that are equipped with this feature. If the feature is not activated, you will see a page where you can enter the license key, if you already have one, for your BladeCenter unit, as shown in the following illustration.

If the feature is activated, you will see the open fabric manager configuration page, as shown in the following illustration.

Note: Open Fabric Manager is not a standard management module feature; it is an extra cost feature that requires a license key. To obtain license keys for features that you have purchased for your BladeCenter unit, go to http://licensing.datacentertech.net. This website contains an overview of the BladeCenter licensing process. Once you obtain a license key, you need to install it on the advanced management module ("License Manager" on page 181 for information). See the *BladeCenter Open Fabric Manager* documentation for more detailed information.

Use the Open Fabric Manager to enable and set addressing for hardware adapters, including the MAC addresses of network interface cards and worldwide node names (WWNN) and worldwide port names (WWPN) of Fibre Channel (FC) host bus adapters. You can use this feature to assign virtual addresses for blade bays in each BladeCenter unit. When a blade server is inserted into a blade bay, with Open Fabric Manager enabled for that blade bay, the Open Fabric Manager configuration is automatically assigned to the blade server, and the blade server starts to use the addresses automatically. You can select up to four types of address; Ethernet, Fibre Channel, SAS, Virtual NIC; and the maximum number of blade offsets to support (0 through 3) when multi-width blade servers are installed in the BladeCenter unit.

You can configure the Open Fabric Manager for up to 100 BladeCenter units.

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:

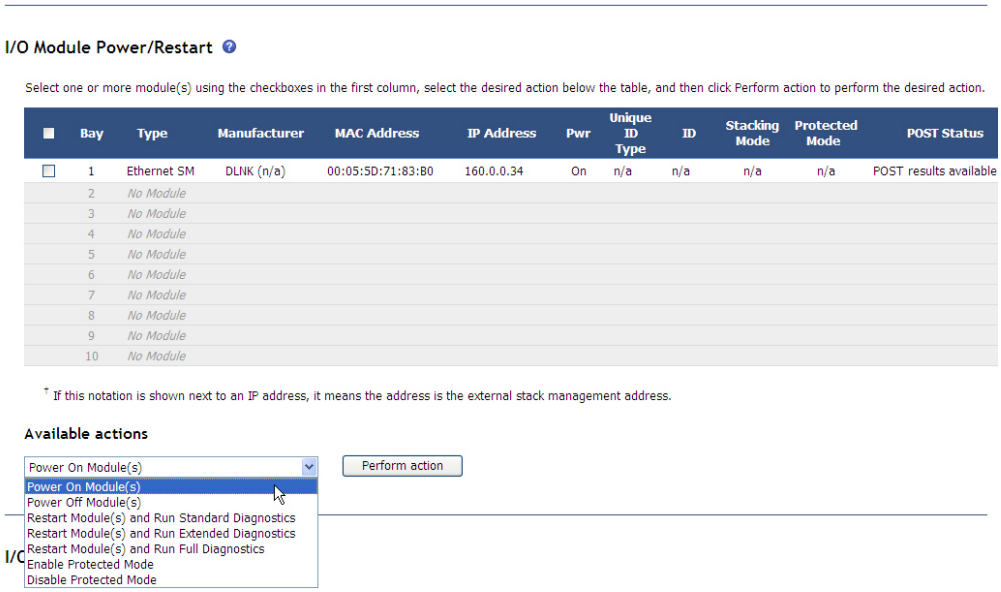
- "Admin/Power/Restart"
- "Configuration" on page 141
- "Firmware Update" on page 146

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 for an advanced management module.



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
- Enable or disable protected mode for an I/O module that supports this feature. When protected mode is enabled for an I/O module, settings for that I/O module cannot be configured through the management module; all I/O-module configuration must be performed through the management interface that is provided by the I/O module. After you enable or disable protected mode through the management module, you must also enable or disable the feature through the I/O-module management console and restart the I/O module. The I/O module retains the protected-mode state that is set in the I/O-module management console, even if it is restarted or moved to a different BladeCenter unit. See the documentation for your I/O module for information.

Note: The BladeCenter S unit supports the RAID serial-attached SCSI (SAS) module, a unit with two subsystems: a SAS switch and a RAID controller. If this device is installed, the I/O Module Power/Restart page is modified as follows:

- The **MAC Address** and **IP Address** columns shows the MAC addresses and IP addresses of both subsystems.
- The **Pwr** column supports a third status message, Shutdown in Progress. This state can occur when a power-off request is issued to the I/O module, which requires additional time to complete pending operations and perform an orderly shutdown. For example, a SAS controller module might need to flush pending I/O operations before it powers off to maintain data integrity.
- The **ID** column shows the VPD identifications of both subsystems.
  - The SAS switch subsystem has one network interface card (NIC) that has a direct Ethernet connection to the advanced management module. The upper IP address label, which ends with "S," is that of the SAS switch subsystem.

– The RAID controller subsystem has one NIC and an indirect Ethernet connection to the advanced management module through the I/O module in bay 1. The lower ID label, which ends with "R," is that of the RAID controller subsystem.

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

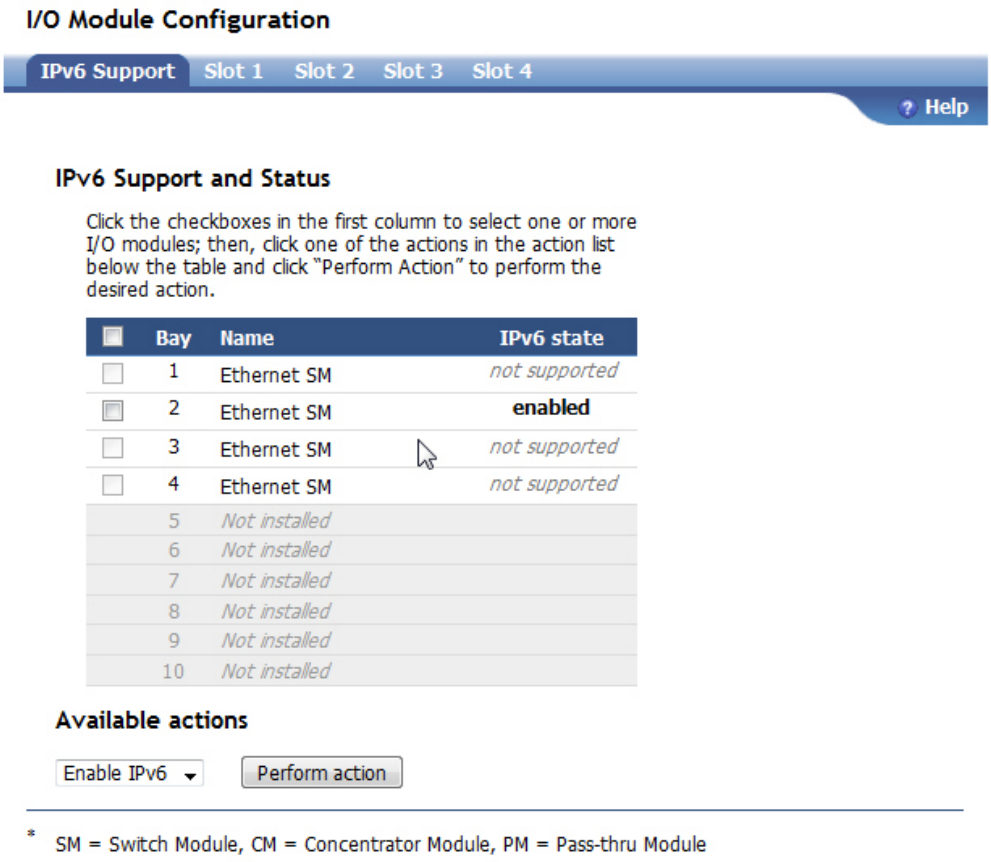
- Fast POST
- External ports

Configuration

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

Note:

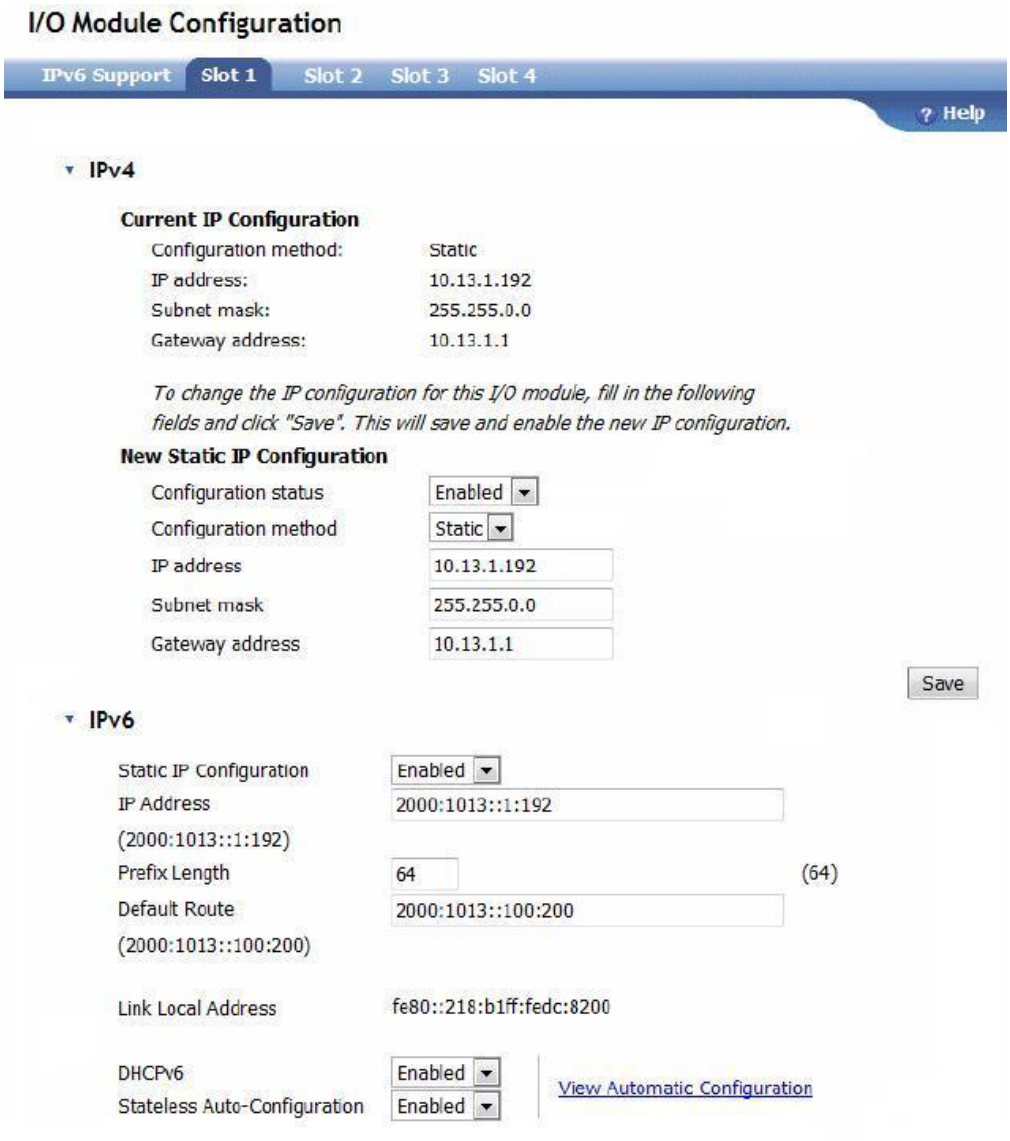
- The content of I/O-module configuration pages varies by I/O-module type. Each page displays only those settings that apply to the I/O module that is installed. Some I/O modules have additional device-specific sub-pages that provide more detailed information and configuration options. See the documentation that comes with the I/O module for device-specific information.
- IPv6 addressing is not supported by all I/O modules.



The I/O Module Configuration page initially displays the IPv6 support tab where you can view and change the IPv6 support state for each I/O module.

There is a tab at the top of the I/O Module Configuration page for each I/O module, indicating the bay (slot) where it is installed. Select a tab to view and change the information for an I/O module. You can also disable or enable static IPv4 and IPv6 addressing for the I/O module in this page.

Note: If the selected bay hosts the RAID SAS module, you can also select this tab to view and change the IP address, subnet mask, gateway address, and VLAN ID of the RAID controller subsystem. This feature is supported by the BladeCenter S unit.



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 view POST results, perform advanced setup tasks, restore an I/O module to the factory default values, ping an I/O module, or start a CLI/web (Telnet) session.

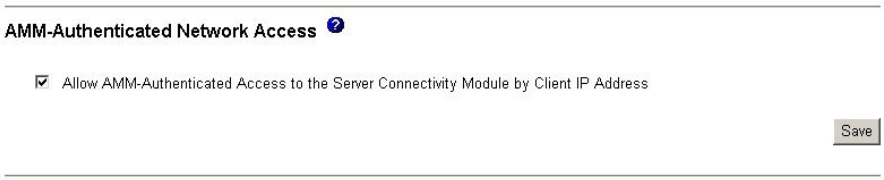
Note: For CLI connection to an I/O module, you must configure your browser to use the Telnet application at your host. The advanced management module does not include a Telnet applet.

If the system includes the RAID SAS module, you also can use this page to ping or establish a CLI (Telnet) session with the RAID subsystem. This feature is supported by the BladeCenter S unit.

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 the letter 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 NAT table in the **Network Protocol Configuration** page.

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.



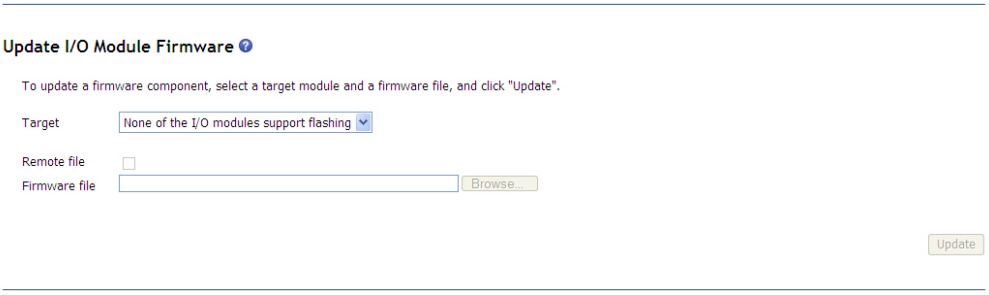
If **AMM-Authenticated Network Access** is enabled, users can connect to a server connectivity module only after the advanced management module authenticates the web interface session login from that client. Access from this client is disabled only when the user logs out or the web interface session times out. This feature enables server connectivity module administrative access to be limited to only those users who are assigned administrative authority for the advanced management module.

If the I/O module indicates that it supports a secure web interface through SSL, the advanced management module can start an SSL session to the I/O module.

See the *Installation and User's Guide* for your BladeCenter unit and "Configuring an I/O module" on page 82 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.



Important: Some cluster solutions require specific code levels or coordinated code updates. If the device is part of a cluster solution, verify that the latest level of code is supported for the cluster solution before you update the code.

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

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

The Remote File method enables you to specify the fully qualified address of the firmware packet file for updating the I/O firmware. The fully qualified address contains a protocol that is supported by the advanced management module followed by a colon and two forward slashes (//), the username and password separated by a colon for login authentication, an @ sign followed by the hostname or IP address, an optional port number, and the full path file name.

Note: If the port number is specified, it must be separated from the hostname (or IP address) by a colon.

The complete format is: *protocol*://*username*:*password*@*hostname*:*port*/*path*/*filename*

The advanced management module supports the following protocols:

- tftp
- ftp
- ftps
- http
- https

An example of a fully qualified address can be:

```
ftp://USERID:PASSW0RD@192.168.0.2:30045/tmp/CNETCMUS.pkt
```

In this example, the ftp protocol will be used for transferring the packet file, the username is `USERID`, password is `PASSW0RD`, host IP address (IPv4) is `192.168.0.2`, port number is `30045`, and `/tmp` is the full pathname to the packet file `CNETCMUS.pkt`.

Some protocols do not need the username, password, and the port number, so the minimum requirement for a fully qualified address can be:

protocol://*hostname*/*path*/*filename*

To update advanced management module firmware by using a remote file, complete the following steps:

1. Check the **Remote File** checkbox.
2. Type in a fully qualified address in the textbox.
3. Click either the **Update** or **Update and Reboot** push button.

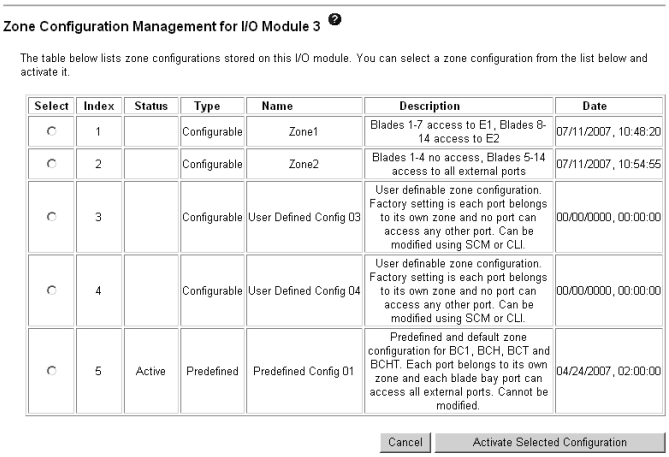
Note: If you are using a hostname instead of an IP address to specify a remote file, make sure DNS is enabled.

Storage Tasks

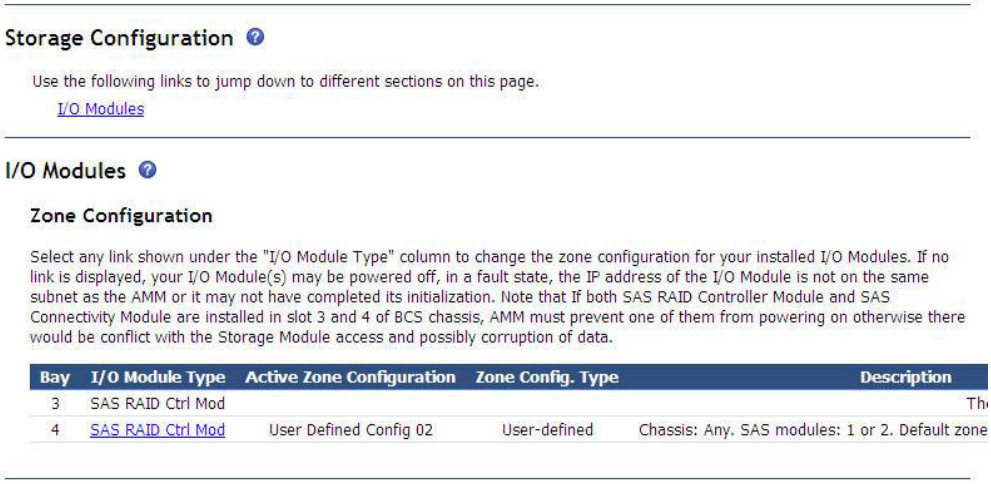
The **Storage Tasks** pages only appear when the advanced management module is installed in a BladeCenter unit that also has storage components or certain types of I/O modules installed.

Select a component from the **Storage Configuration** section to view and modify its storage configuration settings. These settings are available only when a storage device is installed in the BladeCenter unit; if no storage components are installed, the **Storage Configuration** section are not displayed.

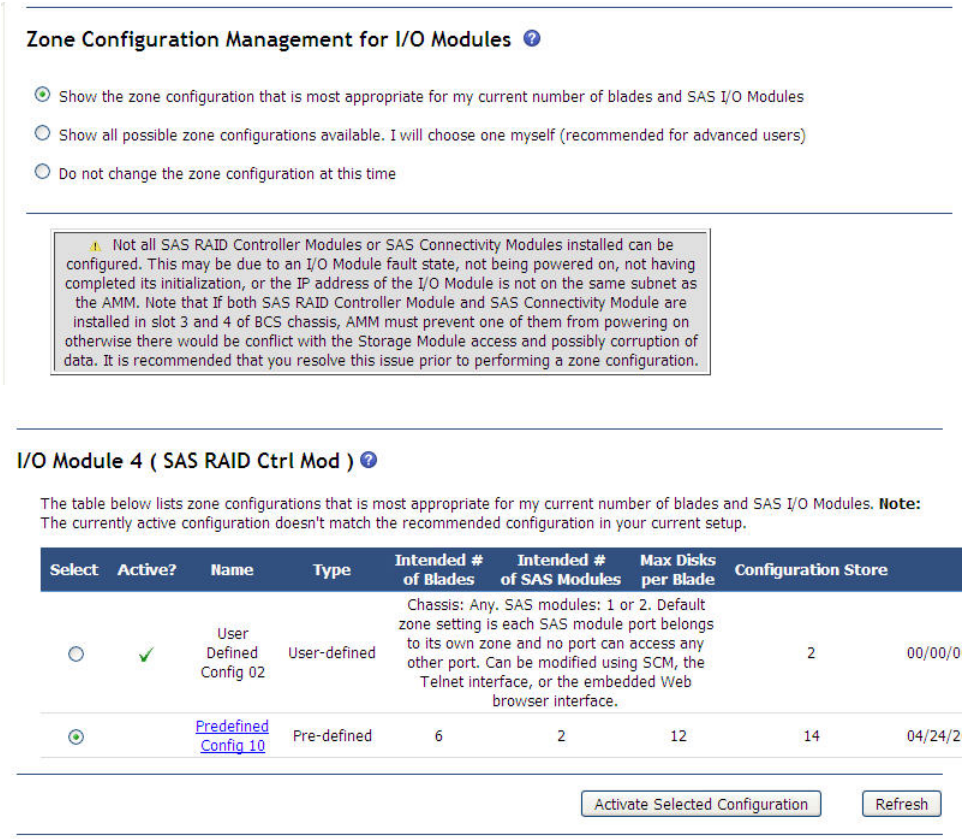
The following illustration shows an example of the available storage configuration settings for a SAS connectivity module. See the documentation for your storage device for detailed information and instructions for configuring the device.



The following illustration shows an example of storage configuration settings for a BladeCenter S unit.



To change the zone configuration for an installed I/O module, click on its link. This will take you to the page you can use to manage the configuration for I/O modules and the optional SAS RAID feature.



When both RAID and non-RAID storage modules are installed, only one module can be powered-on at a time and have its zone configuration managed. If multiple SAS modules are installed and both are working, make sure that the default setting

is used to apply the same zone configuration to each SAS module. To apply different zone configurations, use the separate zone configuration tables for the SAS Modules.

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
- Communication settings for the advanced management module serial port
- The management-module Ethernet connections for remote console and for communicating with the I/O modules
- Settings for the following protocols:
  - File Transfer Protocol (FTP)
  - Lightweight Directory Access Protocol (LDAP)
  - Network Time Protocol (NTP)
  - Secure Shell (SSH)
  - Server Service Location Protocol (SLP)
  - Simple Mail Transfer Protocol (SMTP)
  - Simple Network Management Protocol (SNMP)
  - SMASH Command Line Protocol (CLP)
  - Syslog protocol
  - TCP command mode protocol
  - Telnet protocol
  - Trivial File Transfer Protocol (TFTP)
- Settings for Secure Sockets Layer (SSL) and Secure Shell (SSH) security
- Security settings such as data encryption and account security

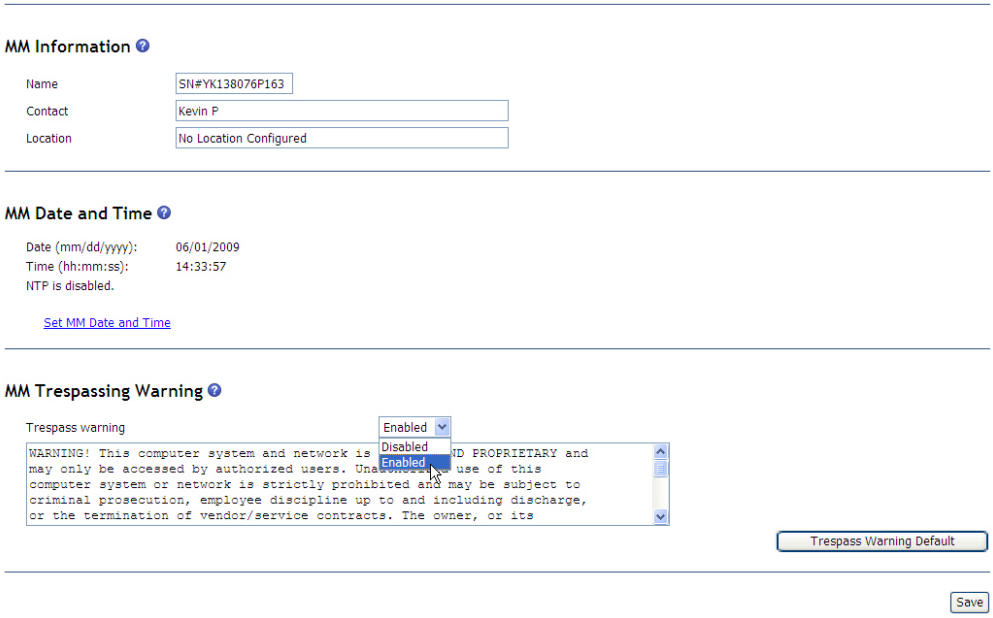
This also includes performing the following tasks:
- Backing up and restoring the management-module configuration
- Updating the management-module firmware
- Restoring the default configuration
- Restarting the management module
- Switching from the primary management module that is currently active 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

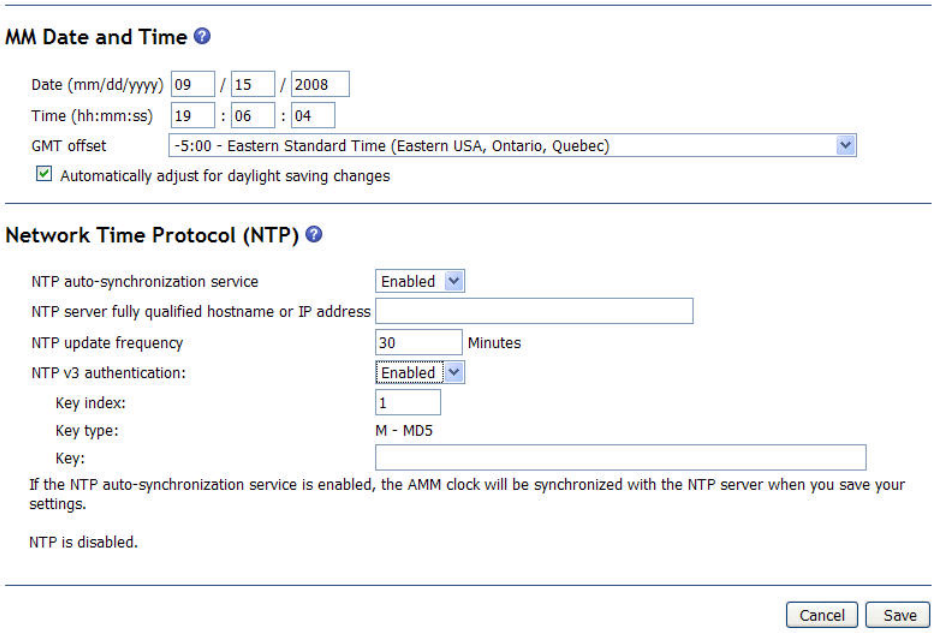
Select **MM Control → General Settings** to enter identifying information, such as time, date, and location.

The following illustration shows the General Settings page for an advanced management module.



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, including network time protocol (NTP) settings for the advanced management module. NTP settings enable automatic synchronization, and set the NTP server IP address, the update frequency, and how often the management module connects.



- 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 23 and "Configuring SMTP" on page 27 for additional information.

Login Profiles

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

The following illustration shows login profiles settings for an advanced management module.

Management Module Login Configuration

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

Login Profiles
Group Profiles
Account Security Management

Login Profiles

To configure a login profile, click a link in the "Login ID" column.

	Login ID	Role	Active Sessions	Last Login	Password Compliant	Days Until Password Expires	Dormant	State	Action
1	USERID	C	0	Never	Yes	n/a		Active	Disable
2	kpervell	S	1	06/01/09 11:20:58	Yes	n/a		Active	
3	johnh	S	0	05/21/09 15:58:29	Yes	n/a		Active	
4	~ not used ~								
5	larry	O	0	Never	Yes	n/a		Active	Disable
6	dale	O	0	Never	Yes	n/a		Active	Disable
7	~ not used ~								
8	~ not used ~								
9	hfuser	O	0	Never	Yes	n/a		Active	Disable
10	~ not used ~								
11	~ not used ~								
12	andrew	O	0	02/13/09 10:44:43	Yes	n/a		Active	Disable

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).

For advanced management modules, the following information is also shown:

- Users that currently are logged in to the management module.
  - Click the **Active Sessions** column heading to view detailed information about each logged-in user or to terminate a logged-in user's session.
  - Click the user **Login ID** to change a password and to set the maximum number of sessions that the user can have open at the same time.
- The date and time that each user last logged in.
- An indication of whether the user password is compliant with the current password policy that is set for the BladeCenter unit.
- The number of days that remain before each user password expires.
- An indication of whether a user profile is dormant (has not been used for a period of time that is specified by the inactivity alert period). The user must log in to recover from a dormant state.
- The state of each user profile: active or disabled. You can manually enable or disable operator and custom profiles by clicking a push button in the **Action** column.

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. For an advanced management module, these settings are configured in the **Account Security Management** 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:

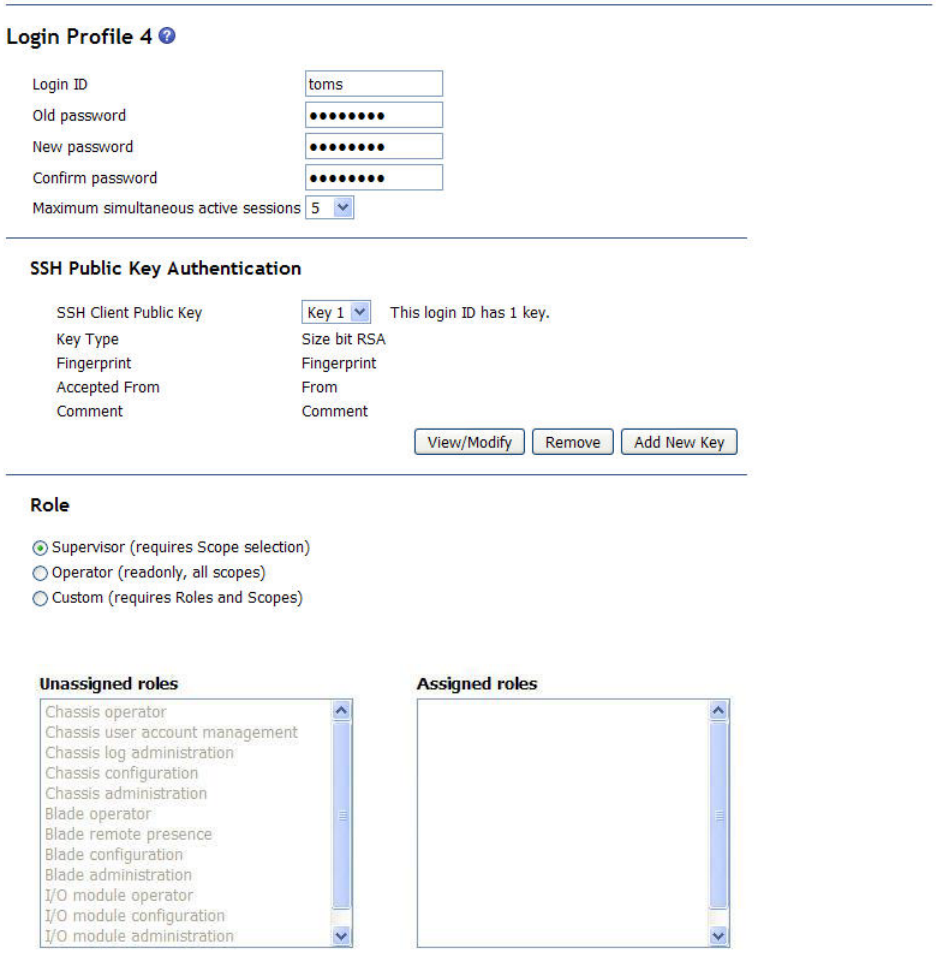
- Login ID
- Password (requires confirmation)
- Role or Authority Level (default is Operator or Read-Only)

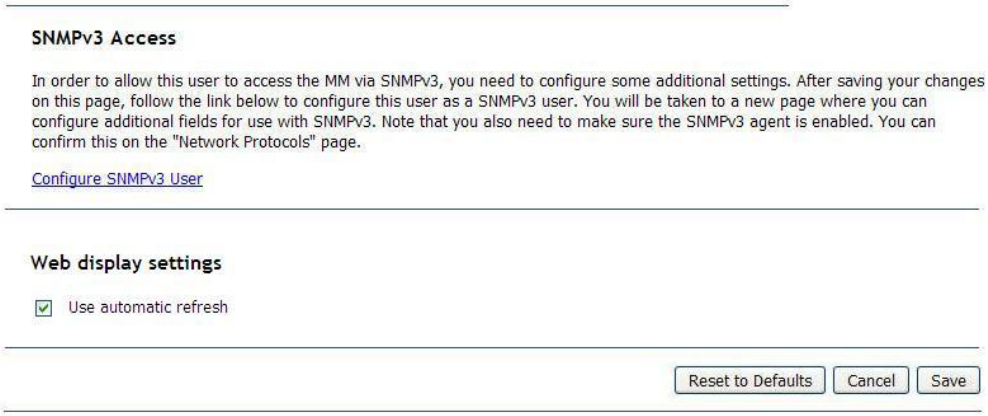
  Defines the command areas that a user can access, according to the user's access scope. Roles or authority levels might vary according to the type of BladeCenter unit that you are using and the management-module firmware version that is installed.
- Access Scope

  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 illustrations show the user profile settings.





Click **Configure SNMPv3 User** to perform additional user configuration that is required for SNMPv3 (see “Configuring SNMP” on page 23 for instructions). If automatic refresh for **Web display settings** is enabled for a user profile, all advanced management module user interface web pages that have auto-refresh capability will be automatically refreshed during web sessions for the user. If automatic refresh is disabled, there will be no automatic refresh for web sessions of this user.

The SSH Public Key Authentication section of the Login Profile page provides for adding, removing, viewing, or modifying the user's SSH public keys. As the Login Profile page is opened on the advanced management module, a summary of key information is displayed for the first key, if any, that is installed for the login profile. If more than one key is installed for the login profile, select the key that you want to view, modify, or remove from the list.

If no keys have been installed for this Login Profile, the only available push button is **Add New Key**.

Use the next page to import a public key, or paste the key data and install one.

The advanced management module accepts SSH public keys that are formatted as OpenSSH-formatted public keys. Keys that are generated by the OpenSSH

ssh-keygen program are acceptable. The length of the key can be up to 4096 bits. Key types ssh-rsa and ssh-dss are accepted. Normally, the key does not contain carriage return or line-feed characters, but these are acceptable when key data is pasted into the **Key Data** field. RFC4716-formatted keys cannot be imported through the web interface. Use the CLI to import RFC4716 formatted keys. The accepted key format contains up to four fields, as follows:

```
< Accepted From specification > < key type > < key data > < comment >
```

The `< Accepted From specification >` and `<comment>` parameters are optional. You can use a space character or tab character to separate the fields.

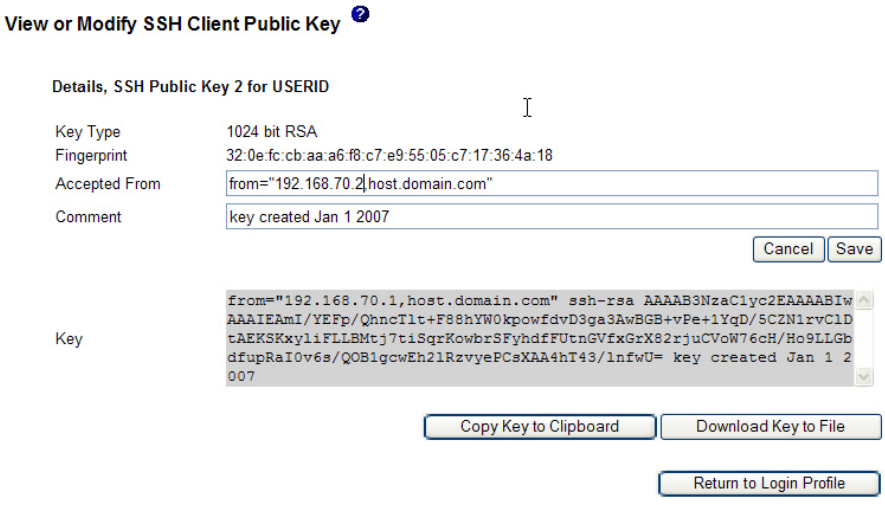
<Accepted From specification>
If this parameter is not used, the SSH public key is accepted from any host. If this parameter is used, it specifies the set of remote IP addresses and host names that can use this SSH public key to authenticate for the login profile. The format of the Accepted From specification is `from=`*`pattern-list`*.

<key type>
The key type must be either ssh-rsa or ssh-dss.

<key data>
The key data consists of displayable text characters. White-space characters, such as the space, tab, and line-feed, are not supported.

<comment>
This parameter can contain text information about the key. You can use this information to help track the various installed keys. The comment field is not used in the authentication process.

If the user has a public key, click **View/Modify** to view or export the selected key. You can also use this page to modify the Accepted From specification and Comment for the selected key.



The fields on this page have the following functions:

Key Type
This field displays the number of bits in the key and the key type (DSA or RSA).

Fingerprint
This field displays a 128-bit MD5 fingerprint of the installed key.

Accepted From
If this field is blank, the SSH public key is accepted from any host. If this field is not blank, it specifies the set of remote IP addresses and host names that can use the SSH public key to authenticate.

Comment
This field can contain text information about the key. The administrator can use this information to help track the various installed keys. The comment field is not used in the authentication process.

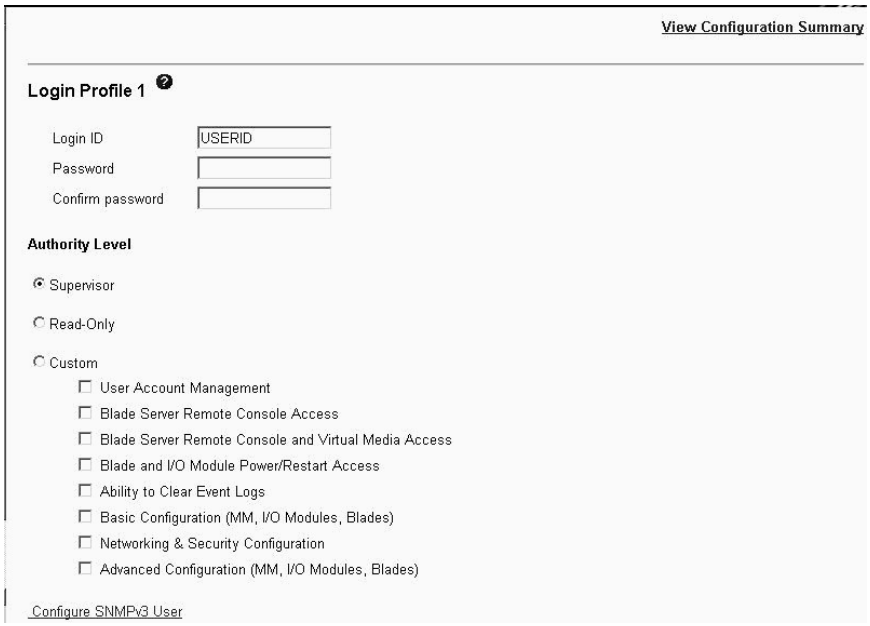
You can update the Accepted From specification on this page by typing the new specification in the field and clicking **Save**. The format of the Accepted From specification is

`from=`*`pattern-list`*

where pattern-list is a comma-separated list of host names and IP addresses.

Each host name or IP address can contain wildcard characters * (asterisk) or ? (question mark), where the asterisk matches any string of characters and the question mark matches any single character. If a host name or IP address is preceded by ! (exclamation point), the key will not be accepted from a host that matches the host name or IP address. DNS must be enabled on the management module if host names are used in the Accepted From specification. The purpose of the Accepted From specification is to optionally increase security: public key authentication by itself does not trust the network, name servers, or anything (but the key). However, if an intruder somehow steals the private key that is associated with an installed public key, the key enables the intruder to log in from anywhere in the world. This additional option makes using a stolen key more difficult. In addition to the key, the name servers, routers, or both would need to be compromised also.

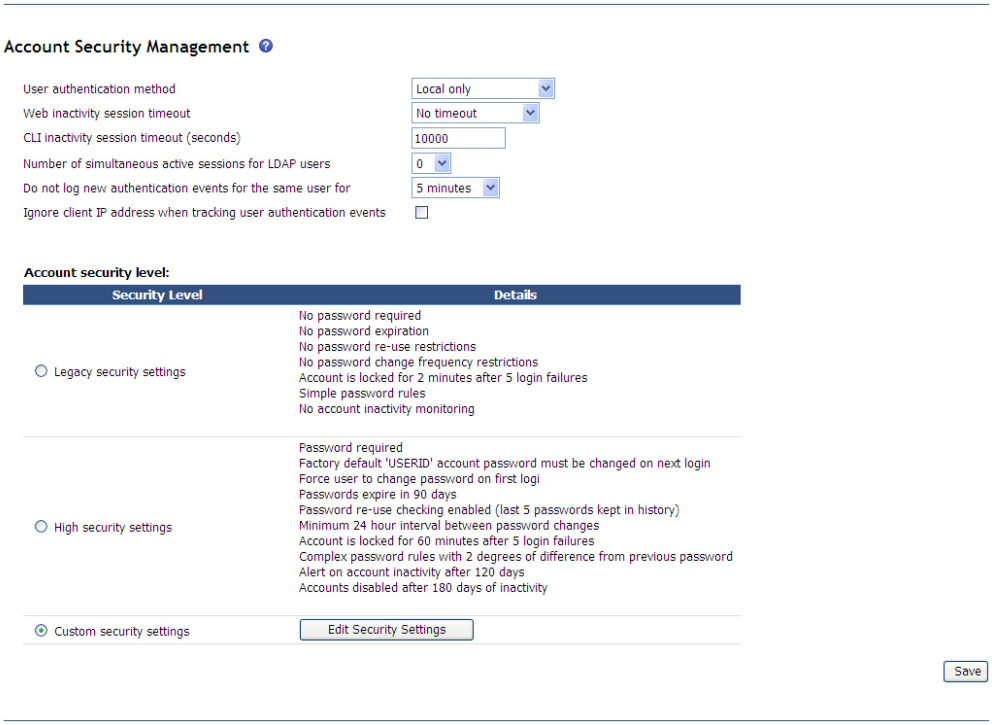
The following illustration shows user profile settings for older versions of management-module firmware.



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 functions. 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.

The following illustration shows the **Account Security Management** area for the advanced management module.



You can modify the following settings:

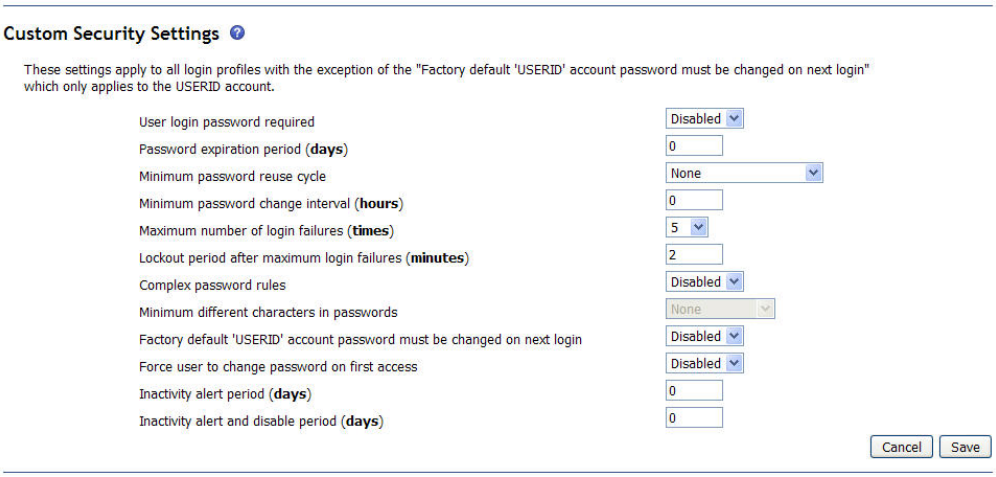
- The user authentication method (local, LDAP, or both).
- The session inactivity timeout for both the web and command-line interfaces.
- The number of simultaneous active sessions for LDAP users. This value applies to all LDAP users and specifies how many concurrent sessions each LDAP user can have. The minimum value is 1, and the maximum value is 20. A value of 0 means that there is no session limit for the user login profile.
- Whether to log new authentication events for the same user for a specified interval. Some scripts that access the management module can generate a large amount of user login and logout activity, which can then fill up the management module event log with login/logout events. Use this field to suppress the logging of some or all of these login/logout events. Select **Log all** to log all user login/logout events. Select **Log none** to stop logging these events completely. Use the other options to set the time period during which a user must be inactive before a new login entry is added to the event log. For example, if you select **5 minutes** and an SNMP script has a user logging in to the management module every minute, only the first login is logged. This is a global setting that applies to all access methods and all users.
- Whether to ignore the client IP address when tracking user authentication events. This check box is unavailable if **Log all** or **Log none** is selected. Otherwise, this check box is available, and you can use it to specify whether a second login by the same user from a different client shall be considered new activity for logging purposes. If the check box is selected, the second login will not be considered new activity; otherwise, it is considered new activity. For example, if **5 minutes** is selected in the **Do not log new authentication events for the same user** field, this check box is selected, and a script has a user logging in to the advanced management module every 3 minutes from two alternating clients, only the first login is logged. However, in the same scenario, if this check box is not selected, every user login is logged, because the user

accesses the advanced management module from each client IP address every 6 minutes. This is a global setting that applies to all access methods and all users.

- The account security level that is to be applied to all user profiles. Two choices with preset values are available, along with a custom settings choice that enables individual values to be modified.
- The minimum password change intervals. This is a security feature that limits how often users can change their passwords.

  Note: If account security settings require passwords, an event log entry is created for each user that does not have SNMPv3 access settings configured for password use.

The following illustration shows the **Custom Security Settings** for the advanced management module.

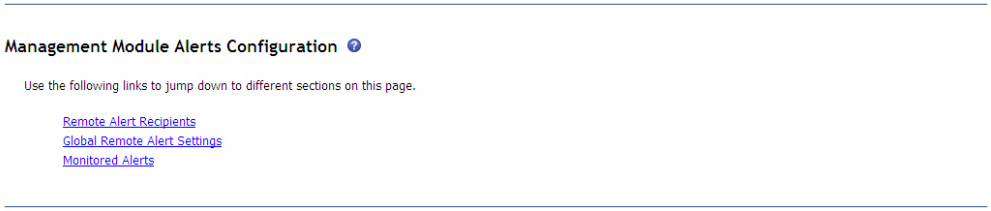


Note: The **Minimum password change interval** setting is a security feature that limits how often users can change their passwords. This setting can be used to prevent a user from changing passwords in rapid succession and afterwards reusing an old password.

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

Alerts

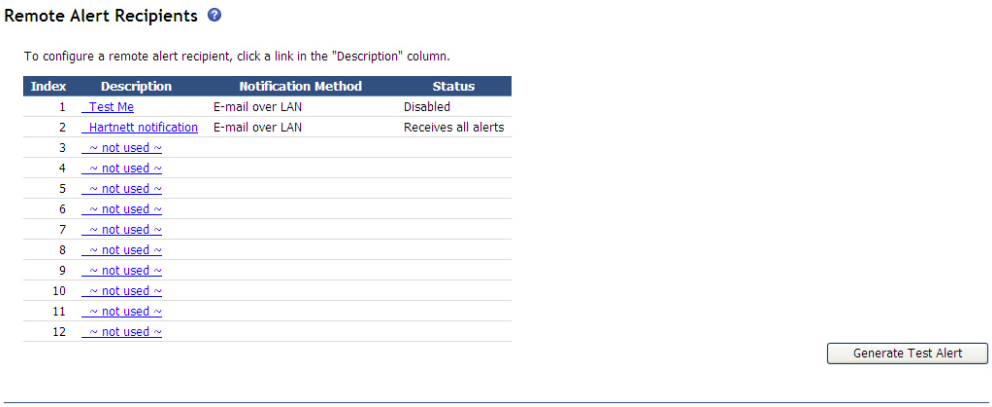
Select **MM Control → Alerts** to manage the process of notifying remote users about specified events in the BladeCenter system.



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

- Define remote alert recipients
- Define global remote alert settings
- Define monitored alerts
- (BladeCenter S and BladeCenter T units only) Manage the passive air filter reminders

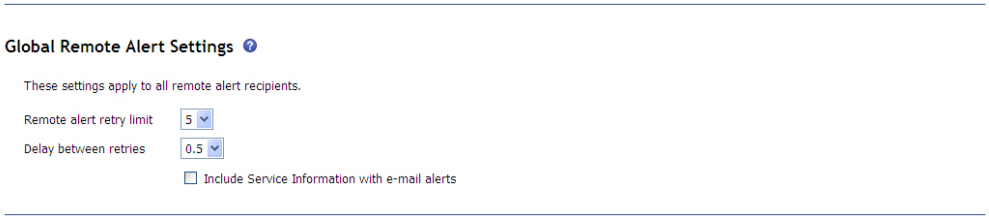
Select **Remote Alert Recipients** to view a list of all users who must be notified about system events. Click a user name to display a secondary page where you can specify which event notifications are sent, how they are sent (SNMP, email, or IBM Systems Director), where they are sent (email address),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



Notes:

- IBM Systems Director (previously known as Netfinity Director or IBM Director) is a systems-management product that comes with the BladeCenter unit. To configure the remote alert recipients for IBM Systems Director over a LAN, the remote alert recipient must be an IBM Systems Director-enabled server.
- IBM Systems Director receives all of the alerts from the advanced management module, even if no alerts are selected on the web page under **Monitored Alerts**.
- A recipient who uses the IBM Systems Director (comprehensive) notification method receives all alerts that are generated by the advanced management module, regardless of whether the type of alert is enabled.

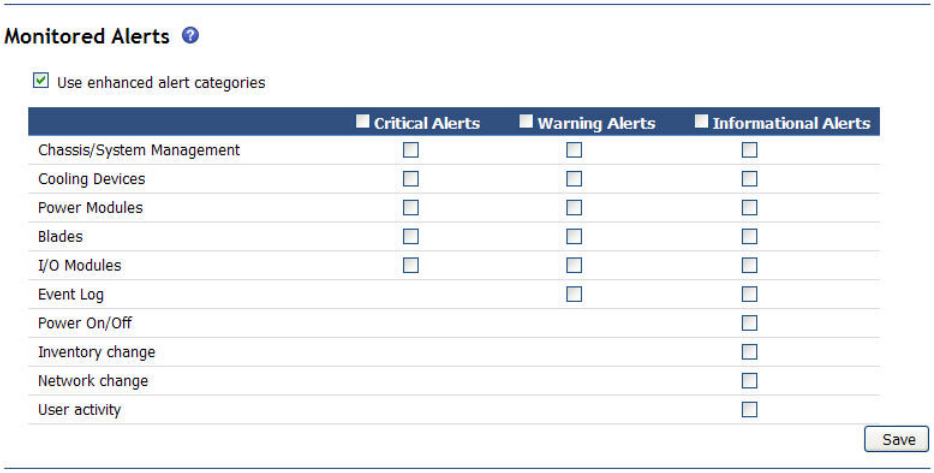
Select **Global Remote Alert Settings** to specify how many times the system attempts to send an alert, how long of a delay is observed between retries, and whether to include the service information with the email alerts.



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.

Note: The old (legacy) alert categories have been replaced with redefined enhanced alert categories. If the **Use enhanced alert categories** check box on the Monitored Alerts page is not selected, the advanced management module handles traps and alerts in the same way as before, but the settings can no longer be modified. If this check box is selected, the currently set old categories migrate into the new categories. Alert monitoring should transition to use of enhanced alert categories. Once this check box is selected and the alert categories are migrated, the **Use enhanced alert categories** check box is no longer displayed and it is impossible to return to the old (legacy) categories.

The following illustration shows a Monitored Alerts page for an advanced management module.



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
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

In the **Passive Air Filter Reminder** section, you can manage air filter reminders for BladeCenter S and BladeCenter T units. Filter reminders for the BladeCenter HT unit are handled automatically. See “Passive air filter reminder” on page 85 for additional information about air-filter reminders for BladeCenter T and BladeCenter HT units.

To request a periodic notification that it is time to change a BladeCenter S unit air filter, select the **Remind me to change this filter in** checkbox; then, select a reminder interval. The following illustration shows the **Passive Air Filter Reminder** section for BladeCenter S units.

For BladeCenter T units, the air filter reminder interval is set to six months and cannot be changed. You can perform one of the following filter-management options:

- **Disable**: Air filter management services are turned off (no air filter alarms or events are generated).
- **Enable**: The six months of service reminder schedule and fouled-filter detection (BladeCenter T and BladeCenter HT units only) are turned on.
- **Restart**: Air filter management services are reset (service reminder schedule is set to generate an air filter reminder after the specified interval).

Serial Port

Select **MM Control → Serial Port** to configure communications settings for the advanced management module serial port.

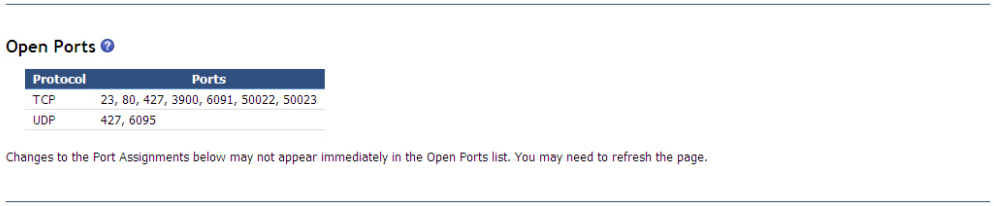
You can configure the serial port settings for baud rate, error checking parity, and the number of stop bits. Connections that are made using the advanced management-module serial port can access only the management-module CLI and the Serial over LAN (SOL) feature. See the *BladeCenter Advanced Management Module Command-Line Interface Reference Guide* for information about using the serial port.

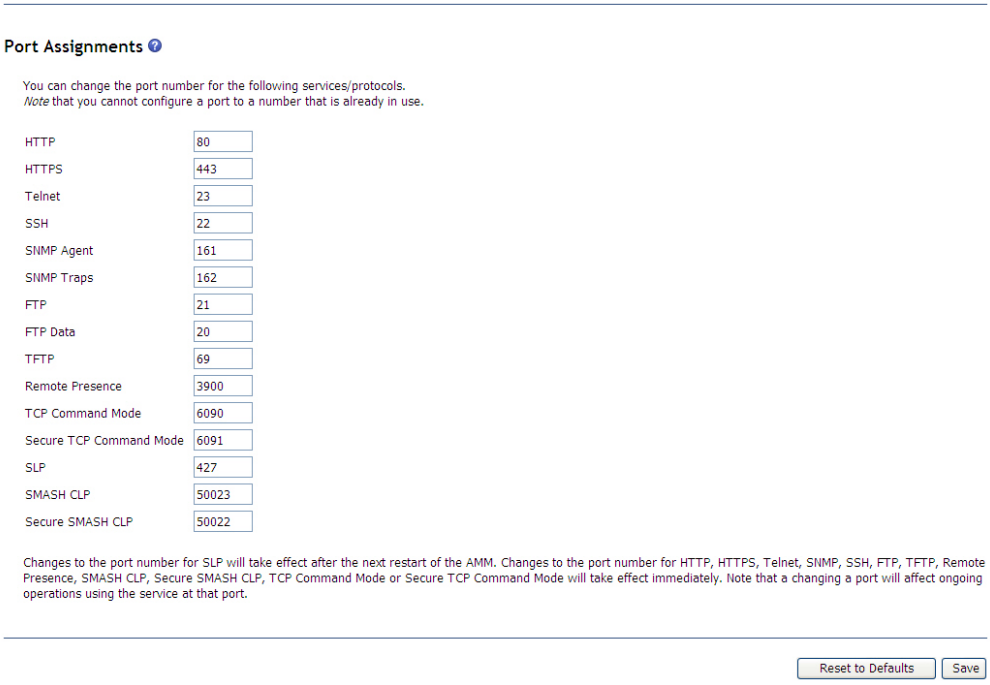
Click **View Configuration Summary** to display the configuration settings for all BladeCenter users and components.

Port Assignments

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

The following illustration shows port assignment settings for an advanced management module.





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. Fixed ports that are used by the management module are listed in Table 5 on page 165. Some ports can be modified by only some management-module types.

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

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
FTP	21	Listen port of the management-module FTP server
FTP Data	20	Data port of the management-module FTP server
TFTP	69	Management-module TFTP server
Remote presence	3900	Remote disk, storage, and KVM operations
SLP	427	UDP Service Location Protocol (SLP) connection
TCP command mode	6090	IBM Systems Director commands using TCP/IP **Note:** IBM Systems Director might not be able to locate the advanced management module using TCP Command Mode if this port number is changed.

Table 4. User-configurable management-module ports (continued)

Port name	Default port number	Purpose
Secure TCP command mode	6091	IBM Systems Director commands using TCP/IP **Note:** IBM Systems Director might not be able to locate the advanced management module using Secure TCP Command Mode if this port number is changed.
SMASH command-line processor	50023	Management-module SMASH command-line protocol over Telnet
Secure SMASH command-line processor	50022	Management-module secure SMASH command-line protocol over SSH

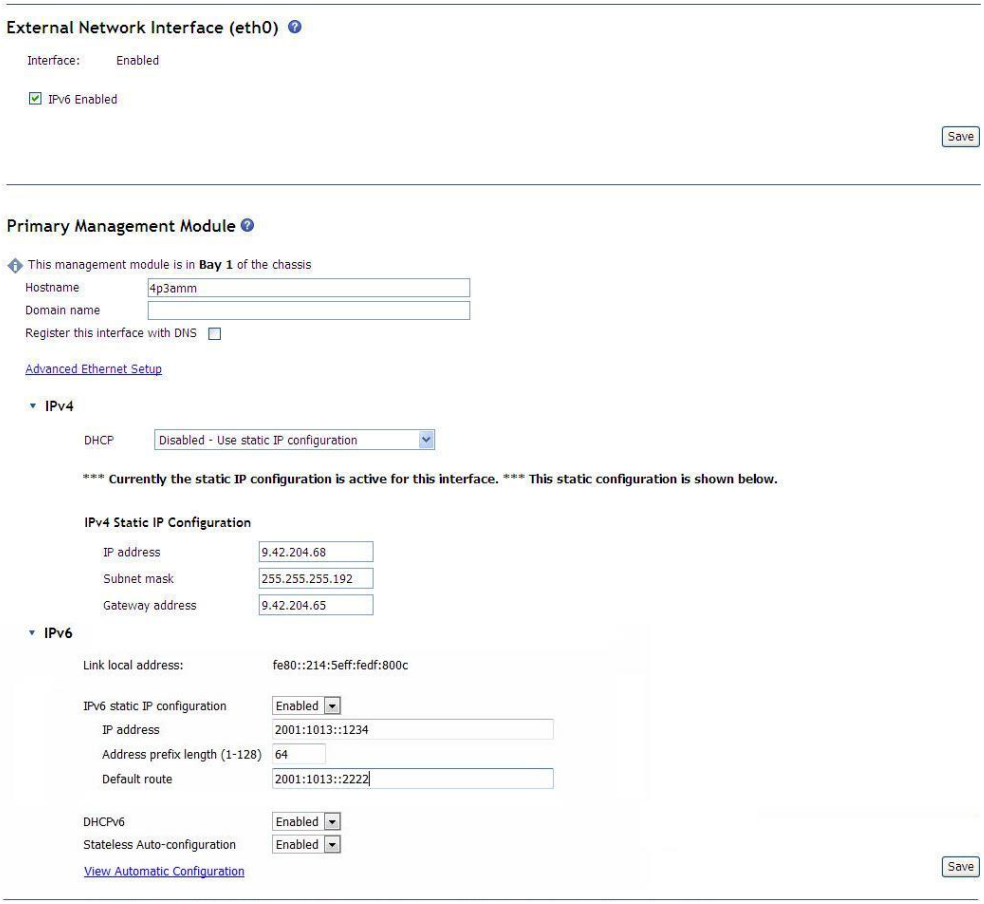
Table 5. Fixed management-module ports

Port number (fixed)	Purpose
25	TCP email alerts
53	UDP Domain Name Server (DNS) resolver
68	DHCP client connection using UDP
13991	IBM Systems Director alerts using UDP

Network Interfaces

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

The following illustration shows the Network Interfaces page for an advanced management module.



Attention: Once IPv6 has been enabled, disabling it or updating advanced management module firmware to a level that does not support IPv6 addressing causes all IPv6 connectivity to be lost. Services and interfaces that are configured for IPv6 operation might not function properly and you will need to reconfigure these services and interfaces.

Select **Network Interfaces** to configure the management-module Ethernet interfaces. For the advanced management module, you can configure only the external Ethernet interface that is used to communicate with the remote management and console. The internal Ethernet interface for the advanced management module has no user-configurable settings.

The advanced management module supports both IPv4 and IPv6 addressing. IPv4 addressing is always enabled and IPv6 is enabled by default. In the **External Network Interface (eth0)** section, if the **IPv6 Enabled** checkbox is not selected, IPv6 addressing is disabled for the BladeCenter unit and you will see an additional checkbox to suppress display of IPv6 information. You must click **Save** for any changes to take effect. The status of the internal (eth1) Ethernet connection for the primary management module is Enabled and cannot be changed.

Note: If IPv6 is enabled, at least one of the IPv6 configuration methods (IPv6 static, DHCPv6, or stateless auto-configuration) must also be enabled and configured.

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 **Primary Management Module** section displays information about the interface for the primary management-module remote management and console port.

Note: If your BladeCenter unit supports redundant management modules and you plan to use this feature with both management modules set to use the same external IP address, disable DHCP and DHCPv6 and configure and use a static IP address. This action must be performed for both IPv4 and IPv6, as appropriate. (The IP configuration information is transferred to the standby management module automatically when it is needed.)

- The following areas of the **Primary Management Module** section apply to both IPv4 and IPv6 addressing:
  - **Hostname** field: (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).
  - **Domain name** field: The domain name of the management module that is used in conjunction with a dynamic domain name server (DDNS).
  - **Register this interface with DNS** checkbox: If checked, the configured DNS servers (see "Network Protocols" on page 170) will also be considered DDNS servers and domain name information will be sent to them.

  Click **Advanced Ethernet Setup** to view and configure the data rate, duplex mode, maximum transmission unit (MTU), and locally-administered MAC address for this interface. The burned-in MAC address field for the external interface is read-only.

  For the advanced management module, you can enable or disable the management-module physical or logical uplink failover features by using the **Failover on loss of physical network link** and **Failover on loss of logical network link** fields. If the external network interface of the primary management module fails, the uplink failover features force a failover to the standby management module, if one is installed, after the specified network failover delay. For an advanced management module, you also can specify the IP address that the management module uses to check the status of its logical network link. The IP address should be for a reliable device on the same physical LAN as the advanced management module. If no IP address is specified, the advanced management module uses the advanced management module gateway IP address, if it is configured. The advanced management module can also listen passively for a routing multicast address to determine if the network is active.
- The following areas of the **External Network Interface (eth0)** section apply to IPv4 addressing:

– **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)

  Note: If the management-module DHCP setting is set to **Try DHCP server. If it fails, use static IP config.**, the management module uses the static IP address when the DHCP server is not available during management-module startup. When this occurs, the IP address might not be reachable if multiple management modules were started with the same static IP address.
– **IPv4 Static IP configuration**: Configure this information only if DHCP is disabled.
  - **IP address**: The IPv4 IP address of the management module 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**: The subnet mask must contain four integers from 0 to 255, separated by periods, with no spaces. The default setting is 255.255.255.0
  - **Gateway address**: The IP address of your network gateway router 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 that were specified above.
– Click **IP Configuration Assigned by DHCP Server** to view the IP configuration that was assigned by the DHCP server. (This choice is available only when DHCP is enabled.)

• The following areas of the **External Network Interface (eth0)** section apply to IPv6 addressing:

  Note: For IPv6, both DHCPv6 and IPv6 static configuration can be enabled at the same time, each with their own address. Hosts like the advanced management module can have multiple IPv6 addresses.
– **Link-local address**: (read only) A unique IPv6 address for the advanced management module that is automatically generated based on the MAC address (see “IPv6 addressing for initial connection” on page 10 for additional information).
– **IPv6 Static IP configuration**: IPv6 static IP configuration is disabled by default.

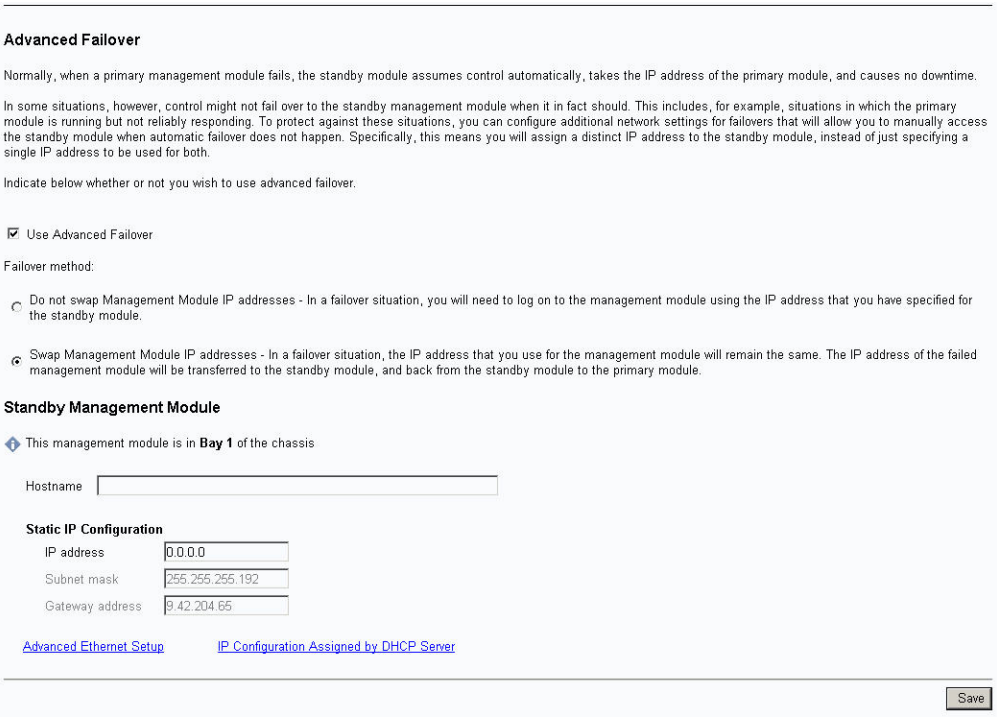
  Note: The advanced management module will not have a fixed static IPv6 address by default. For initial access, users can use either the IPv4 or the IPv6 link-local address.
  - **IP address**: The IPv6 IP address of the management module must be 16 hexadecimal bytes, divided along 2-byte boundaries, delimited with colons, of the form: 2001:0DB8:0000:0000:02AA:00FF:FE28:9C5A.
  - **Address prefix length (1-128)**: The prefix length for the IPv6 address. The address prefix length is not configurable for the standby advanced management module: the same value as the primary advanced management module is used.
  - **Default route**: The IP address of your network gateway router must be 16 hexadecimal bytes, divided along 2-byte boundaries, delimited with colons, of the form: 2001:0DB8:0000:0000:02AA:00FF:FE28:9C5A. The default route

is not configurable for the standby advanced management module: the same value as the primary advanced management module is used.

– **DHCPv6**: Select one of the following choices:
  - **Enabled: Obtain IP configuration from DHCP server** (the default)
  - **Disabled: Not obtain IP configuration from DHCP server**
– **Stateless Auto-configuration**: Automatic configuration of addresses is based on the receipt of Router Advertisement messages. These messages include stateless address prefixes. Stateless auto-configuration is enabled by default.

Click **View Automatic Configuration** to view the DHCPv6 information and stateless auto-configuration addresses assigned to the primary advanced management module. All fields are read-only.

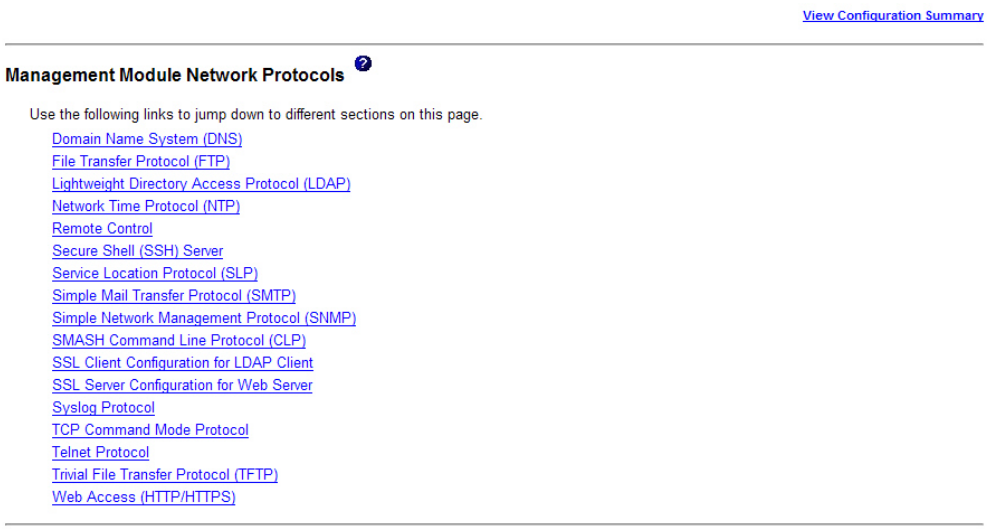
The **Advanced Failover** section sets how the management module behaves when it switches over to the standby management module during failover. It also displays information about the interface for the standby management-module remote management and console port, similar to the **External Network Interface (eth0)** section and **Primary Management Module** section for the primary management module.



Network Protocols

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

The following illustration shows network protocol settings for an advanced management module.



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

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. For an advanced management module, you also can configure the FTP, TFTP, Syslog, and SMASH settings and enable or disable each of the management interfaces (management-module web interface, command-line interface, TCP, and SNMP).

SLP provides a broadcast-based mechanism to query the status of advanced management modules on the network. An advanced management module uses results of these queries to display Remote BladeCenter unit status.

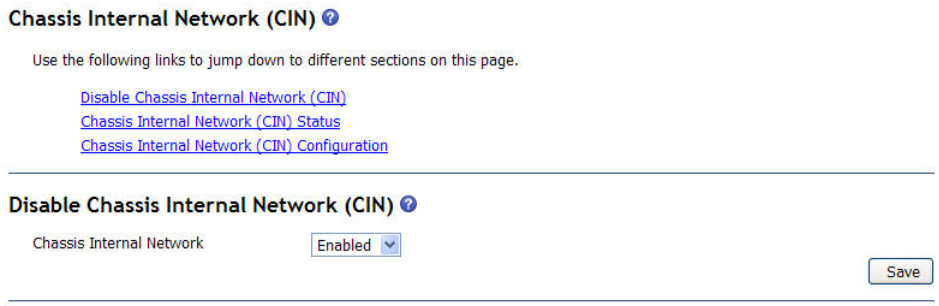
The syslog protocol provides a method for the advanced management module to send event-log messages over the network to one or two syslog collectors. This is useful because the advanced management module event log has a limited capacity and when it is full, it wraps, and the oldest entries are overwritten. By configuring syslog collectors, you prevent the loss of any event history. See “Enabling Syslog” on page 61 for details about configuring the syslog feature and generating test messages.

Note: For an advanced management module, the Telnet interface and SMASH command-line processor also can be enabled or disabled through SNMP and the management-module command-line interface. See the *BladeCenter Advanced Management Module Command-Line Interface Reference Guide* or the *IBM SMASH Proxy Installation and User's Guide* for more information.

Some of the network protocol settings are used during SNMP, SMTP, and LDAP configuration. See “Configuring SNMP” on page 23, “Configuring SMTP” on page 27, and “Configuring LDAP” on page 27 for additional information.

Chassis Internal Network

Select **MM Control → Chassis Int Network** to manage internal connectivity between blade server ports and an internal advanced management module management port.



The Chassis Internal Network (CIN) provides internal connectivity between blade server ports and the internal advanced management module management port so that you can access the management module from a blade server by opening a WEB, CLI or SNMP session.

The communication path is two-way, so that the advanced management module also can use the services on the blade server, including LDAP, SMTP, DNS and NTP (Network Time Protocol).

Use the **Chassis Internal Network (CIN) Status** page to view the status of existing CIN elements.

CIN VLAN ID
The Virtual LAN (VLAN) ID that supports CIN.

CIN IP Address
The IP address that communicates on the CIN. An asterisk (*) after the address indicates that the address was dynamically assigned and is not explicitly configured by the user.

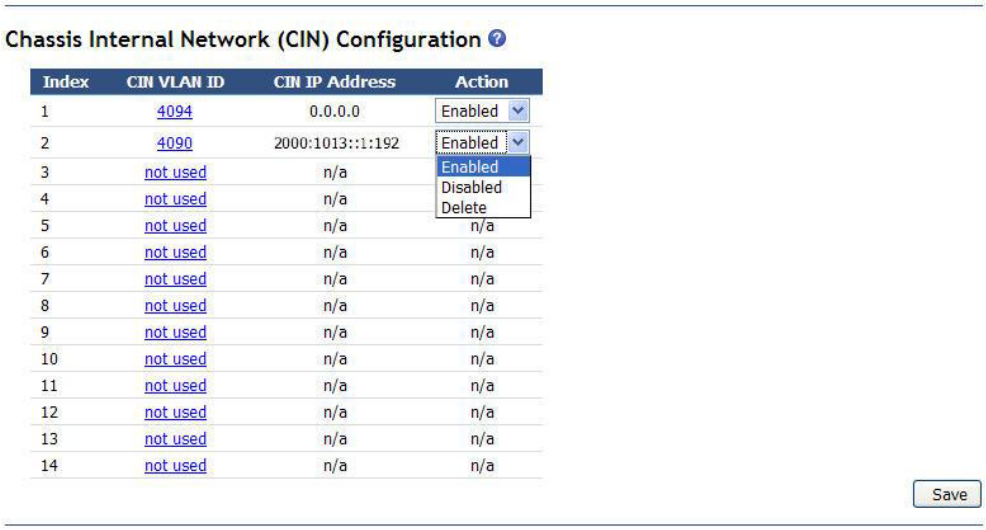
CIN MAC
The MAC address that is associated with the IP address.

Status
The CIN connection status. The following values are possible:

- **Operational**: The advanced management module can ping the CIN IP address.
- **Not Operational**: The advanced management module cannot ping the CIN IP address. Make sure that the blade server and the I/O module are configured correctly and that their configurations are compatible with the

advanced management module. The CIN connection has a status of Not Operational if one of the following conditions exist:
  - The blade server operating system must have an IP host route defined.
  - The I/O modules already have a VLAN defined that contains the port for the blade server and the advanced management module.
- **Disabled**: The CIN configuration has been disabled by an advanced management module administrator.

To find the management module from the blade server, you must assign one or more CIN VLAN IDs (CIN VID) on the **Chassis Internal Network (CIN) Configuration** page.



Each CIN interface to the advanced management module has an associated index number, ID, IP address, and action value.

CIN Index
This is an index of 1 through 14 to identify the CIN configuration.

CIN VLAN ID
This is a number 3 through 4094. These VLAN IDs cannot be the same as the one that is used for SOL/cKVM. A value of **~not used~** indicates that the configuration entry has not been defined. Click a VLAN ID to define the entry.

CIN IP Address
This is the IP address that is enabled to communicate on the CIN. A value of 0.0.0.0 (IPv4) or 0::0 (IPv6) indicates that any IP address can communicate on the CIN. In this case, the advanced management module listens on the CIN VLAN ID and learns the IP addresses dynamically. To restrict the addresses, define each IP address specifically. CIN entries cannot have matching IP addresses, with the exception of 0.0.0.0 (IPv4) or 0::0 (IPv6). Multiple CIN entries with an IP address of 0.0.0.0 (IPv4) or 0::0 (IPv6) are supported, provided that the VLAN IDs are different. The IP address of a CIN entry cannot be multicast or match the advanced management module IP address.

Action
Use this menu to enable, disable, or delete an existing CIN configuration.

Note: You can globally enable or disable CIN. When CIN is disabled, all CIN functions are disabled, even if index entries 1 through 14 are configured.

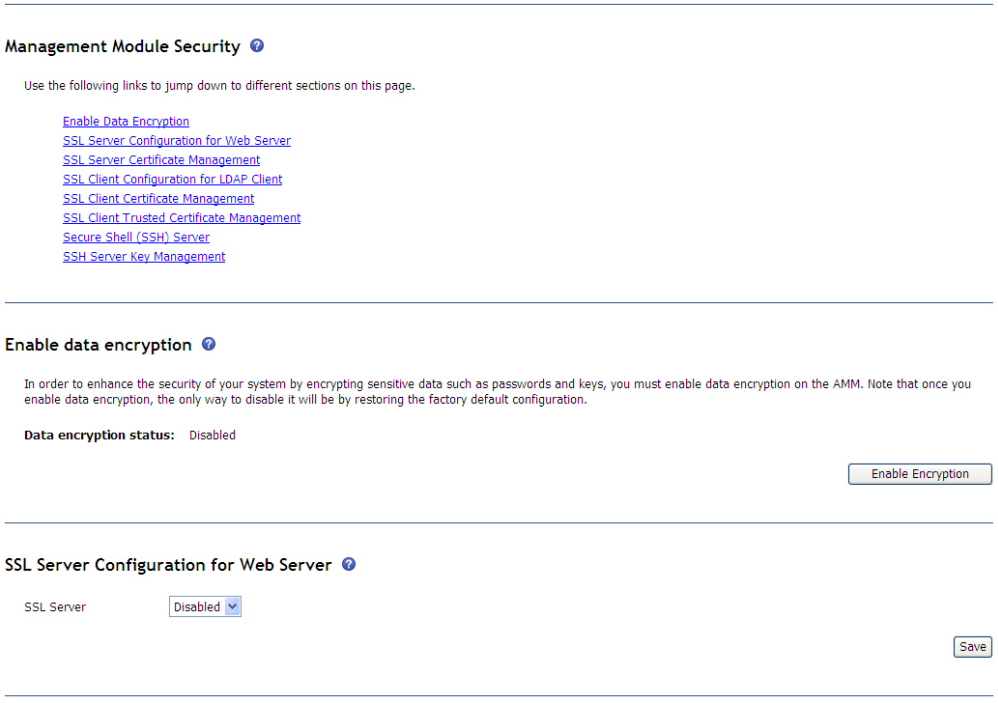
To create a new CIN VLAN configuration, click one of the **~not used~** entries; the **Chassis Internal Network (CIN) Entry Definition** page displayed.

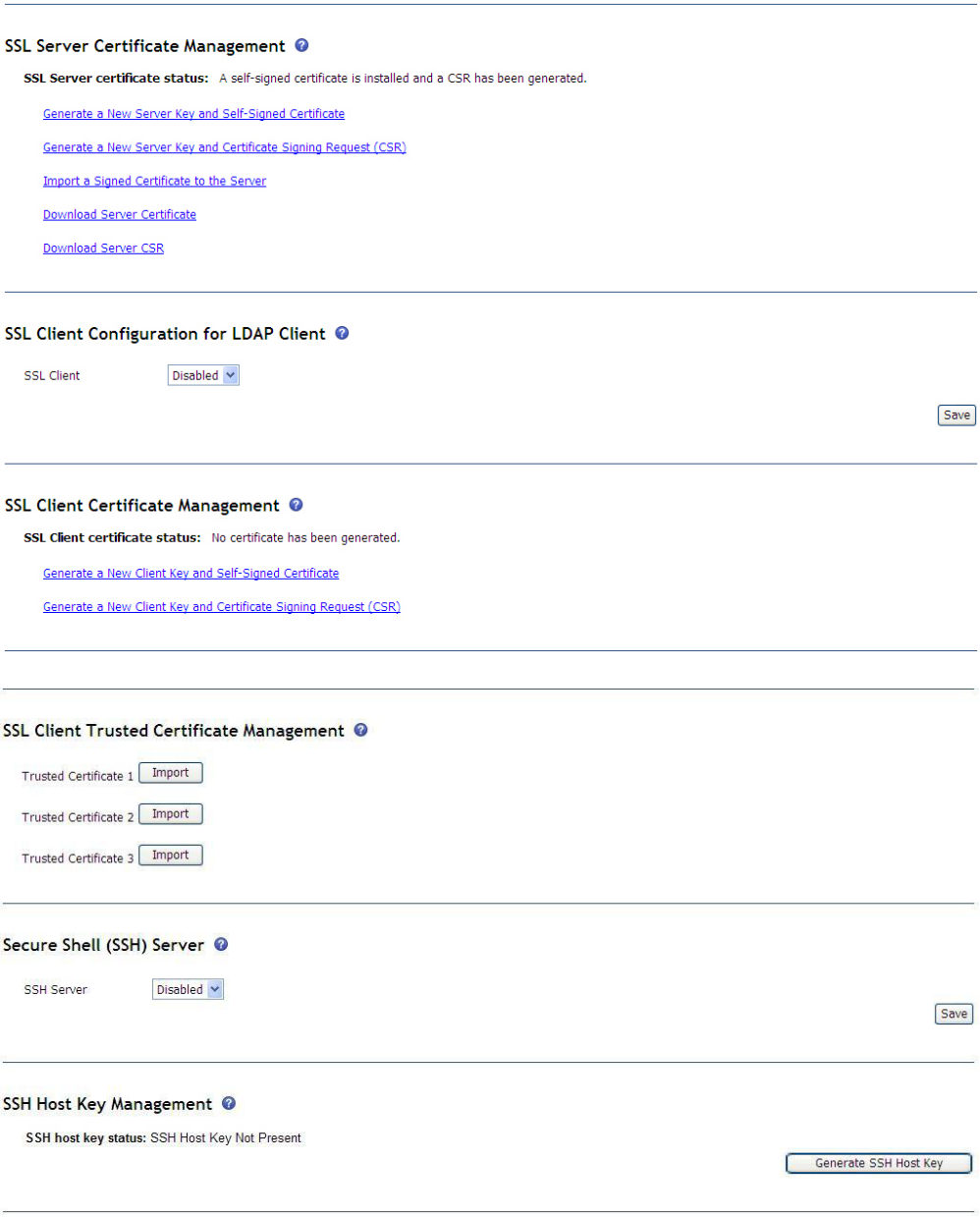
Enter the VLAN ID and IP address; then, click **Save** to add the configuration to the existing CIN VLAN configurations, or click **Cancel** to return to the previous page.

Security

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

The following illustrations show examples of security settings for an advanced management module.



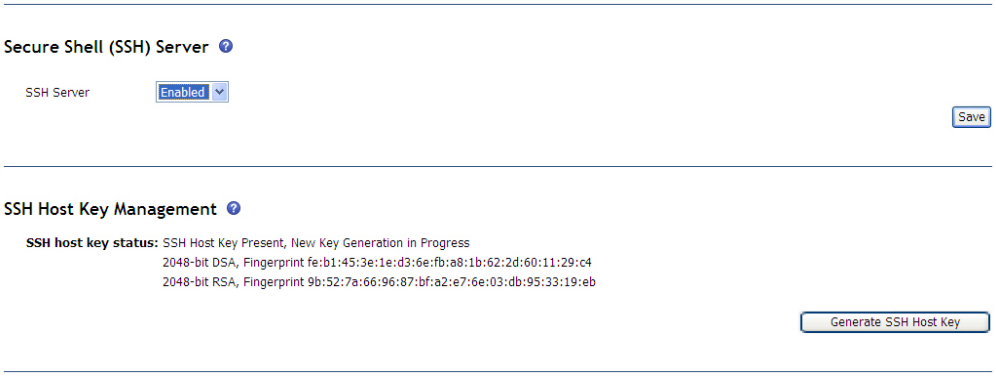


Select **Security** to view or change the Secure Sockets Layer (SSL) settings for the web server and LDAP client and to view or change the Secure Shell (SSH) server settings. You can enable or disable (the default) SSL and select between self-signed certificates and certificates that are provided by a certificate authority (CA). You also can enable (the default) or disable SSH and generate and manage the SSH server key. For an advanced management module, you also can enable or disable data encryption for sensitive data such as passwords and keys. When data encryption is enabled, the only way to disable data encryption is by restoring the management module to its factory default configuration. If data encryption is enabled, installing a management module firmware update that does not support data encryption causes all management module configuration settings to revert to their factory default values.

Notes:

- For an advanced management module, you also can enable or disable SSH by using SNMP and the management-module command-line interface. See the *BladeCenter Advanced Management Module Command-Line Interface Reference Guide* for more information.
- An advanced management module can use installed SSH public keys to enable authentication without using passwords. Up to 12 public keys can be installed to enable user access.
- An advanced management module generates SSH host keys automatically, if no host keys are installed and either SSH or Secure SMASH is enabled.

The following illustration shows the Secure Shell configuration page for an advanced management module.



Some of the security settings are used during SSL, LDAP, and SSH configuration. See "Secure web server and secure LDAP" on page 44 and "Configuring the Secure Shell (SSH) server" on page 56 for additional information.

File Management

Select **MM Control → File Management** to view and manage the contents of the local storage area on the advanced management module.

The following illustration shows the File Management page for advanced management modules.

The **File Management** choice shows a list of files and available space in the advanced management module file system. You can delete files that are stored in the advanced management module. The page displays up to two levels of file

directories and their content. Each directory that is shown in the display is represented by an open folder icon. If there are additional subdirectories below the levels that are being displayed, the directory names of the next level are shown as web links that are represented by closed folder icons. To display the next two directory levels, click a directory name link. There is no depth limit. Use the web browser back button to navigate back up the directory tree two levels at a time or click **File Management** in the navigation pane to go directly to the top of the advanced management module directory tree.

You can upload files to the advanced management module local storage area through FTP or TFTP or by using the management-module Remote Disk feature (see "Using the remote disk feature" on page 70 for information and instructions). FTP and TFTP servers on the advanced management module are enabled through the MM Control > Network Protocols page (see "Network Protocols" on page 170).

To delete a file, select it; then, click **Delete Selected Files**. Click **Refresh** to update the display.

Note:

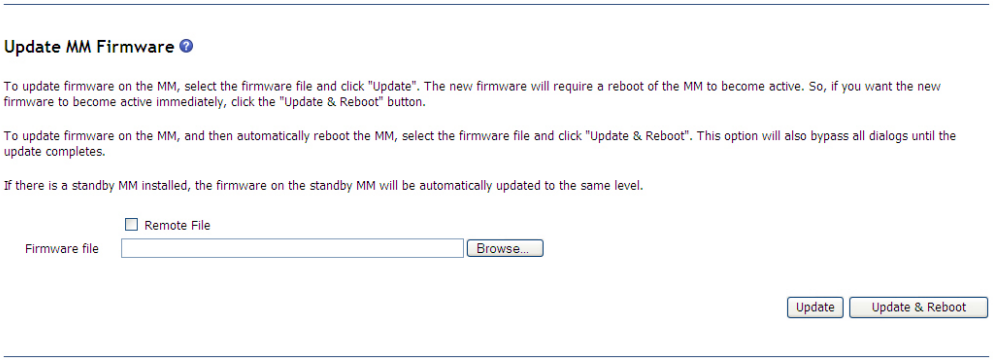
- A user must have Supervisor, Chassis Administrator, Chassis Configuration, Blade Administration, Blade Configuration, I/O Module Administration, or I/O Module Configuration privileges to delete a file.
- Directories cannot be deleted.

Firmware Update

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

Important: Some cluster solutions require specific code levels or coordinated code updates. If the device is part of a cluster solution, verify that the latest level of code is supported for the cluster solution before you update the code.

The following illustration shows the management module firmware update page for the advanced management module.



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/.

The Remote File method enables you to specify the fully qualified address of the firmware packet file for updating the advanced management module. The fully qualified address contains a protocol that is supported by the advanced management module followed by a colon and two forward slashes (//), the username and password separated by a colon for login authentication, an @ sign followed by the hostname or IP address, an optional port number, and the full path file name.

Note: If the port number is specified, it must be separated from the hostname (or IP address) by a colon.

The complete address format is:

protocol://*username*:*password*@*hostname*:*port*/*path*/*filename*

Currently, the following protocols are accepted and understood by the advanced management module:

- tftp
- ftp
- ftps
- http
- https

An example of a fully qualified address is:

```
ftp://USERID:PASSW0RD@192.168.0.2:30045/tmp/CNETCMUS.pkt
```

In this example, the ftp protocol will be used for transferring the packet file, the username is `USERID`, password is `PASSW0RD`, host IP address (IPv4) is `192.168.0.2`, port number is `30045`, and `/tmp` is the full pathname to the packet file `CNETCMUS.pkt`.

Some protocols do not need the username, password, and the port number, so the minimum requirement for a fully qualified address can be:

protocol://*hostname*/*path*/*filename*

To update the advanced management module firmware by using a remote file, complete the following steps:

1. Check the **Remote File** checkbox.
2. Type in a fully qualified address in the textbox.
3. Click either the **Update** or **Update and Reboot** push button. The **Update and Reboot** push button will bypass confirmation windows and automaticall reboot the advanced management module when the flash is completed.

Note: If you are using a hostname instead of an IP address to specify a remote file, make sure DNS is enabled.

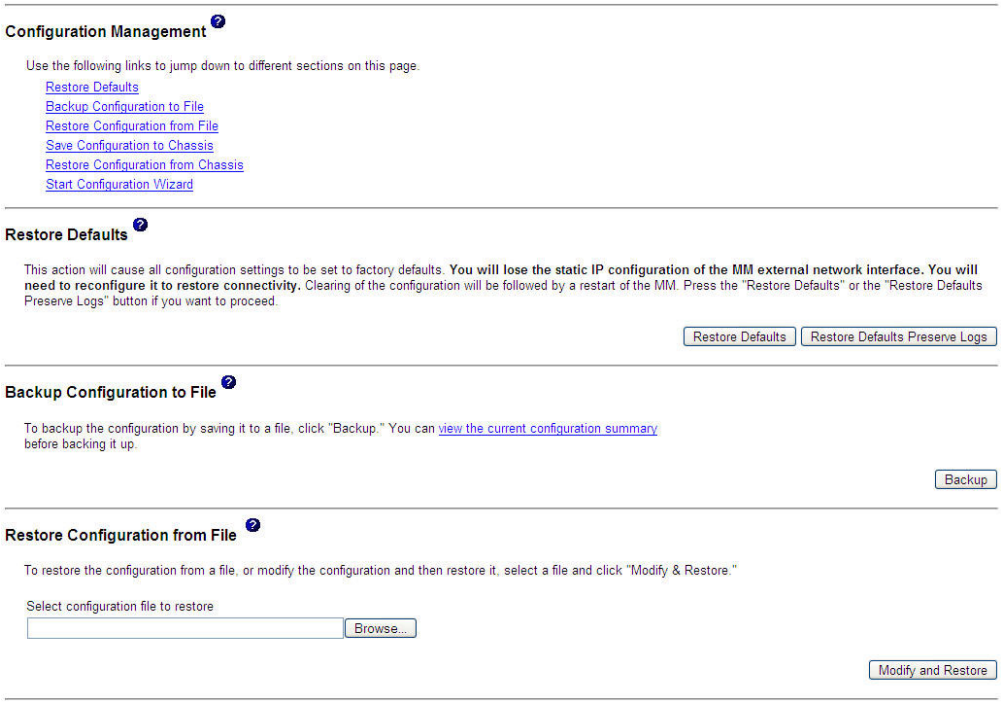
Important: Make sure that the role or command authority level that is set for each user is correct after you update the management-module firmware, because these definitions might change between firmware versions.

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.

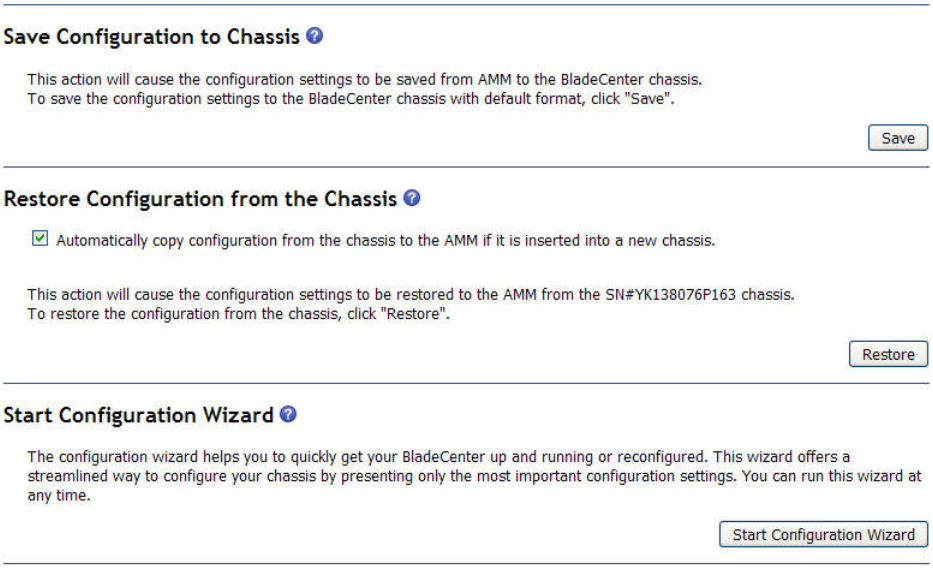
Configuration Mgmt

Select **MM Control → Configuration Mgmt** to back up or restore the management-module configuration. You also can use this page to start the configuration wizard.

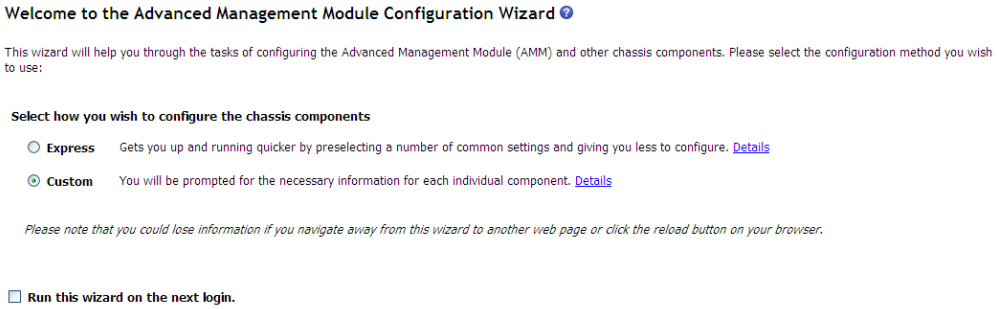


The advanced management module provides several backup and restoration options, including use of a compressed configuration file for BladeCenter units other than BladeCenter H units. (BladeCenter H units compress backups automatically.) When you restore defaults, you can choose to save or discard the management-module event log. See “Using the configuration file” on page 65 for instructions.

You can also store configuration files on the local BladeCenter unit (chassis) and retrieve them from that location.



Click the **Start Configuration Wizard** link to begin a guided setup of an advanced management module. The configuration wizard offers express and custom configuration options.

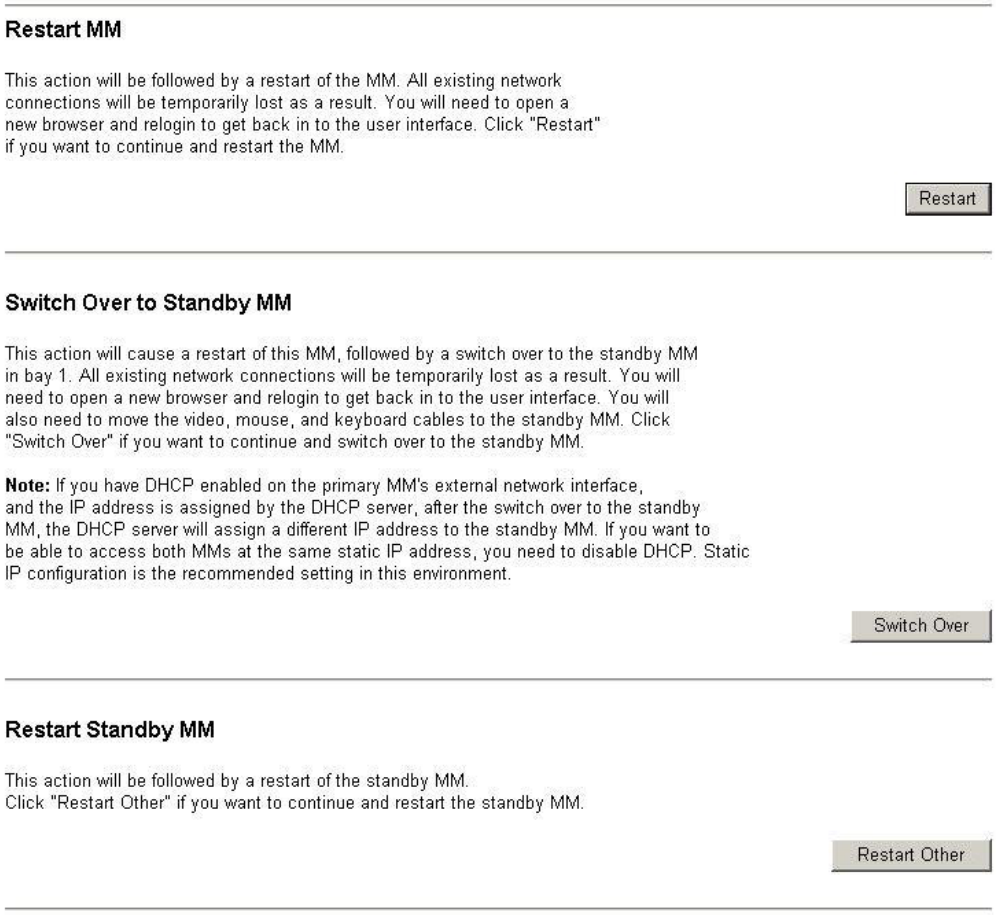


The configuration wizard repackages the information in the other advanced management module pages into a structured flow that facilitates the configuration process. See “Using the configuration wizard” on page 19 for information about using the configuration wizard.

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.

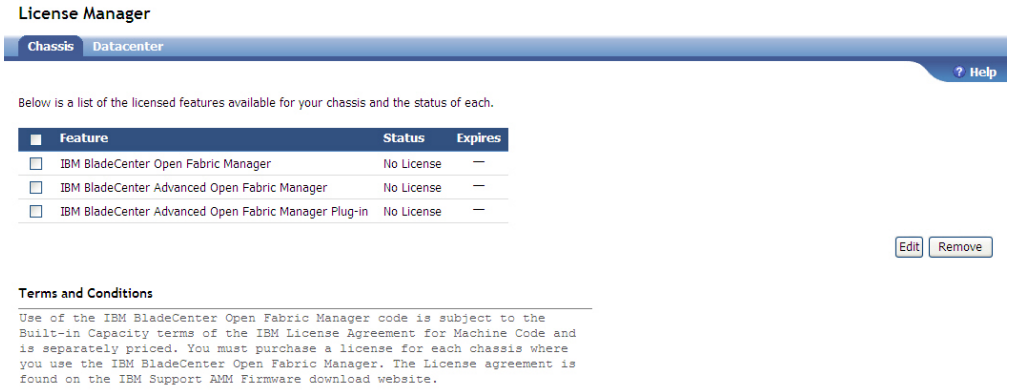
The following illustration shows the Restart MM page for an advanced management module.



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. For an advanced management module, you also can restart the standby management module.

License Manager

Select **MM Control → License Manager** to manage advanced management module features that require a license.



License Manager is used to manage license information for either a single BladeCenter unit or any number of BladeCenter units in a datacenter. Extra cost features, such as Open Fabric Manager, can be used with your BladeCenter unit once you install a valid license key for the feature. More information about how to obtain license keys for features that you purchased can be found at http://licensing.datacentertech.net.

License keys are stored in the advanced management module and are only valid if the advanced management module is installed in the BladeCenter unit that has the correct machine type, model, and serial number. If you install a new advanced management module in the BladeCenter unit or if you restore the advanced management module configuration to defaults, you must reinstall the license keys. For BladeCenter units with primary and redundant advanced management modules, license keys installed in the primary advanced management module are backed up to the redundant advanced management module. For these BladeCenter units the license keys are preserved if one advanced management module is replaced at a time.

The License Manager page initially displays the Chassis tab that shows the status of advanced management module licensed features installed for this BladeCenter unit. It displays the name of the each feature, the number of days left before the license expires, and one of the following status indications for each feature:

No License
The feature is not available. The license entitlement information has not been entered.

Active The licensed feature is available. The license is installed with correct parameters.

Chassis Serial Mismatch
The feature is not available. The license key stored on the advanced management module does not match the machine serial number of the BladeCenter unit.

Chassis Type Mismatch
The feature is not available. The license key entered on the Enter License Information page is not compatible with the BladeCenter unit type.

Expired
The feature is not available. The trial license is expired and is no longer active.

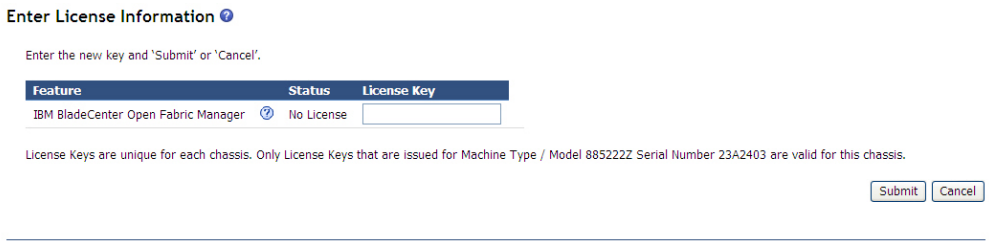
The following license types are available for BladeCenter features:

Permanent
This is the standard license type for purchased features; it has no expiration

60 Day Trial
This license type allows you to use a feature for 60 days from the date that you install its trial license key on the advanced management module.

Transitional
This license type is automatically created for Basic Open Fabric Manager users that upgrade to a level of advanced management module firmware that implements license entitlement checking. The transitional license allows these users to continue using the Basic Open Fabric Manager without disruption. If you have a transitional license, go to http://licensing.datacentertech.net to obtain a permanent license for your BladeCenter unit. Permanent licenses are backed up at this website to protect license keys in the event of loss or hardware failure. Go to http://licensing.datacentertech.net to track licenses for datacenters that have multiple BladeCenter units.

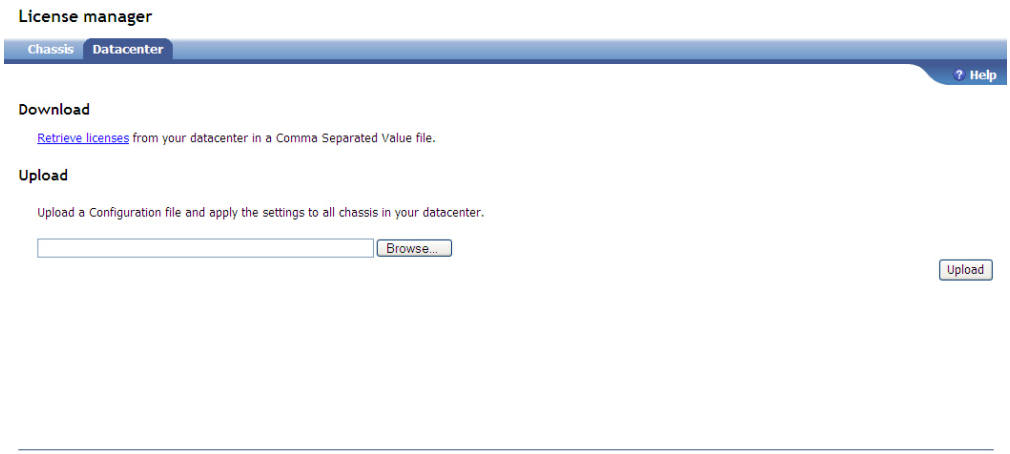
To modify the license information for a feature, select it and click **Edit**. Selecting a feature and clicking **Remove** disables a licensed feature. The following page displays when you edit a feature.



Feature licensing enablement requires entry of the following information:

License Key
A 7-character lowercase alphanumeric string that is unique for the combination of feature, chassis, and license type. License keys can be obtained from the licensing website at http://licensing.datacentertech.net.

On the Datacenter tab you can retrieve and download or upload a configuration file that contains the license information for your datacenter. Both of these operation are necessary to deploy and manage licenses in a datacenter environment that has multiple BladeCenter units.



The download operation locates all of the management modules in a datacenter, creating a license file that contains hardware and license information for each BladeCenter unit, as reported by each management module. This file can be uploaded to the licensing website at http://licensing.datacentertech.net to create or update the record of licensing information for the datacenter. Service Location Protocol (SLP) must be enabled in the “Network Protocols” on page 170 page on each management module in the datacenter to allow data collection. The TCP Command Mode protocol must also be enabled in the “Port Assignments” on page 163 page and the user name and password for the current login session must be valid on all discovered management modules to collect their license status.

The upload operation accepts the specified license file and deploys its license keys to the management modules listed in the file. Using the download and upload operations speeds data collection, license deployment, and eliminates issues associated with manual data entry.

Service Tools

For an advanced management module, select the choices in **Service Tools** to access information that might assist a technician who is servicing the BladeCenter unit.

Service tools choices are:

- "AMM Service Data"
- "Blade Service Data" on page 185
- "AMM Status" on page 186
- "Service Advisor" on page 188

AMM Service Data

Select **Service Tools → AMM Service Data** to view or download information collected in the service data capture file.

Notes:

- If you have activated the Service Advisor feature, this service data capture file is automatically sent to IBM when a serviceable event occurs. See "IBM Service Advisor" on page 75 for more information.
- To send this service data capture file to IBM, click **Manually Email Service Information**.
- For BladeCenter S units, if the RAID SAS module is installed, this page lists vital product data about the battery backup unit.

Click **Save Service Data** to save this service data capture file on your system.

The service data capture file filename is automatically generated and follows the form *ammName*`_YYYYMMDD_hhmmss.tgz`, where:

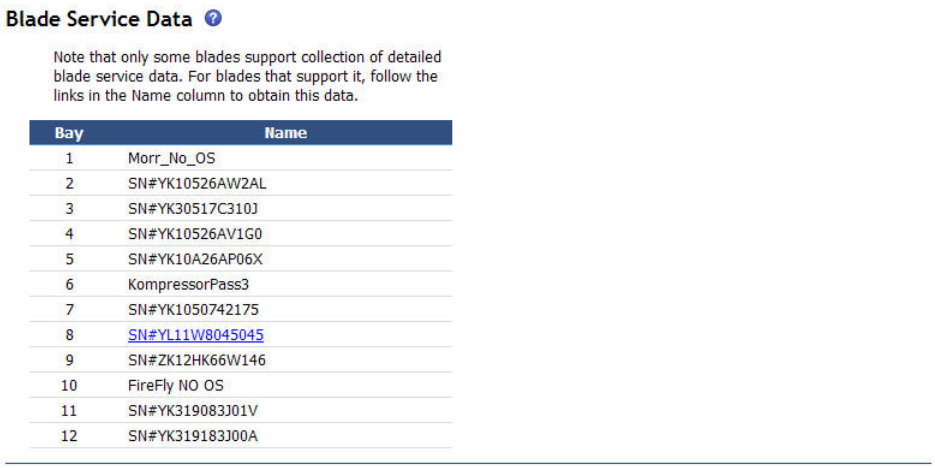
- The *ammName* indicates the name of the advanced management module
- The *YYYYMMDD* indicates the date of service data capture in year-month-day format.

- The *hhmmss* indicates the time of service data capture in hour-minute-second 24-hour clock format.
- The .tgz extension indicates that this is a GZipped Tar Archive file which you can unbundle using common utilities.

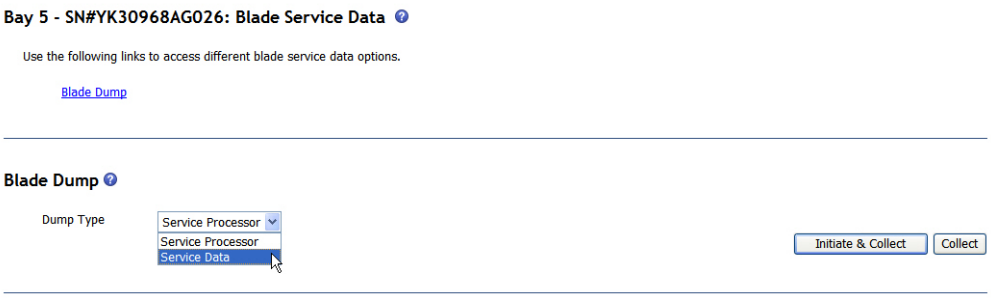
Blade Service Data

Select **Service Tools → Blade Service Data** to view a table of all the blade servers in the BladeCenter unit. The Blade Service Data page is available only if there is at least one blade server in the BladeCenter unit that supports the collection of blade service data.

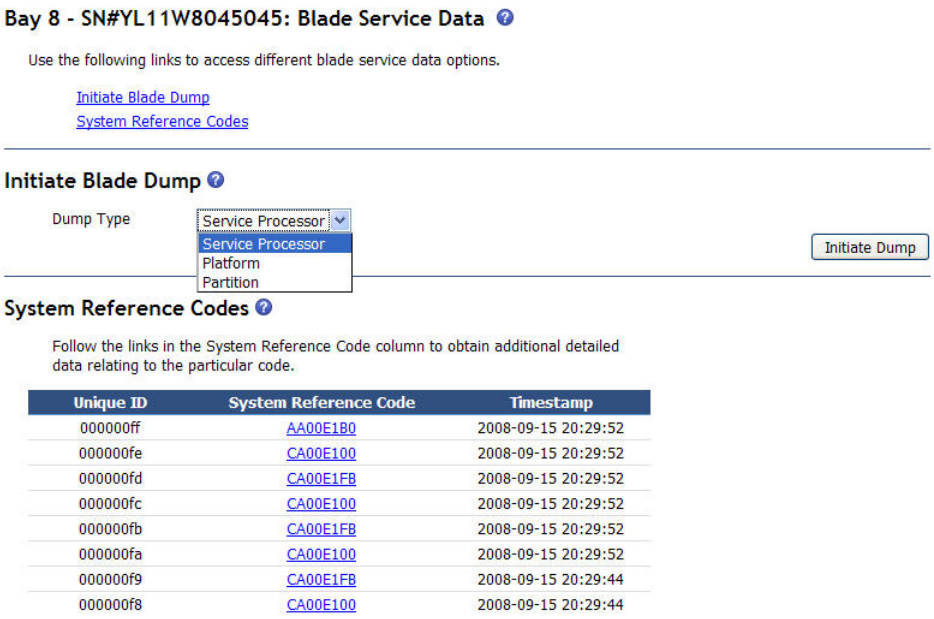
For each blade server that supports the collection of detailed blade server service data, there is a link in the **Name** column. Click the link to manage service data for that blade server. These links are displayed only if there is at least one blade server in the BladeCenter unit that supports the collection of blade server service data.



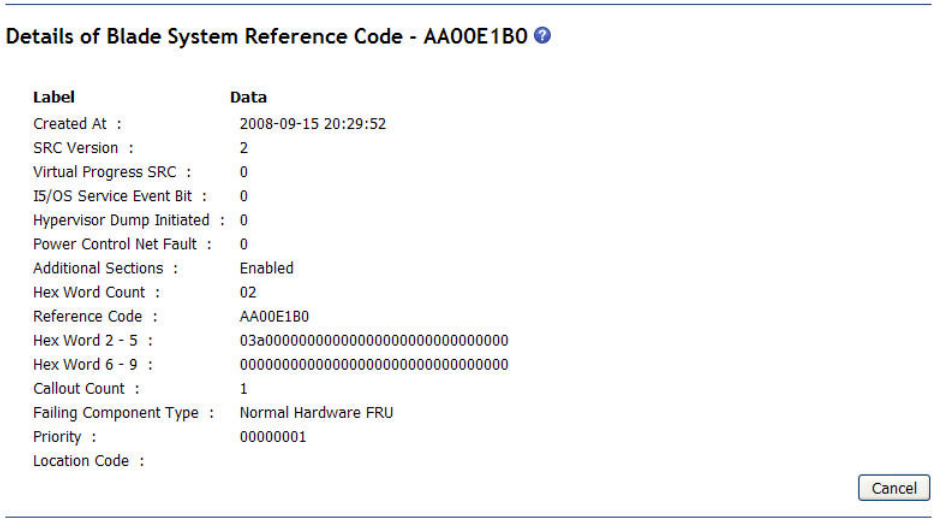
Use the menu in the **Initiate Blade Dump** section to select the type of blade server service data dump that you want to generate; then, click **Initiate & Collect** to dump and display the blade server service data or **Collect** to display the data collected during the last dump. The types of service data that are available vary, based on blade server type. New dumps overwrite existing dump data and can be used by support personnel to diagnose issues. The dump can cause the generation of associated System Reference Codes (SRC) records.



The **System Reference Codes** section displays a table of the 32 most recent system reference codes of a blade server. This interface indicates whether detailed data is available for a particular system reference code.



To show the details of a system reference code, click the system reference code link. A page that contains the details of the selected system reference code is displayed.



The information on this page can be used by support personnel to diagnose issues. See the *Problem Determination and Service Guide* for assistance with interpreting the codes and detailed data.

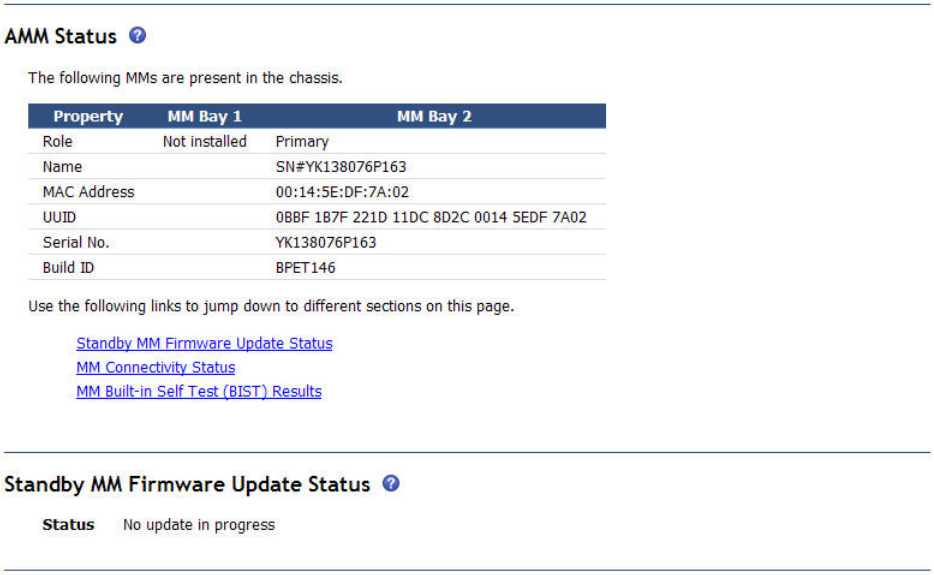
Note: Some blade servers do not support system reference codes.

AMM Status

Select **Service Tools → AMM Status** to view information that uniquely identifies the advanced management modules that are installed in your BladeCenter unit.

Click **Standby MM Firmware Update Status** to view the progress of a firmware update for the standby advanced management module. Click **MM Connectivity**

Status to view the status of management-module connections. Click **MM Built-in Self Test (BIST) Results** to view the results of management-module self-tests.



The **Standby MM Firmware Update Status** section displays the status of the firmware update, versions of the firmware images, percent complete, and estimated time to complete the update of the standby management-module firmware.

Note: The BladeCenter S unit does not support a second (standby) management module; therefore, this category is not on the management-module user interface for the BladeCenter S unit.

The **MM Connectivity Status** section displays the status of connections between the management modules and other BladeCenter components. The status of connections with the primary management module is periodically updated. If a standby management module is installed, its connection status shows the data that was collected the last time the management module was the primary management module; if the management module never acted as primary, no status data is available for it. The **Last Update** field shows when the status information for each management module was collected.

Note: The BladeCenter S unit version of the advanced management module also displays connectivity information for the storage modules.

MM Connectivity Status

Status:
Last update: 6/01/2009 15:37

Module	MM Bay 1 (Primary)	MM Bay 2 (Empty)
Blade 1	Not Installed	
Blade 2	Not Installed	
Blade 3	Not Installed	
Blade 4	Communicating	
Blade 5	Not Installed	
Blade 6	Not Installed	
Blade 7	Not Installed	
Blade 8	Not Installed	
Blade 9	Not Installed	
Blade 10	Not Installed	
Blade 11	Not Installed	
Blade 12	Not Installed	
Blade 13	Not Installed	
Blade 14	Not Installed	
I/O Module 1	Communicating	
I/O Module 2	Not Installed	
I/O Module 3	Not Installed	
I/O Module 4	Not Installed	
I/O Module 5	Not Installed	
I/O Module 6	Not Installed	
I/O Module 7	Not Installed	
I/O Module 8	Not Installed	
I/O Module 9	Not Installed	
I/O Module 10	Not Installed	
Media Tray	Communicating	
Power Module 1	Communicating	
Power Module 2	Communicating	
Power Module 3	Communicating	
Power Module 4	Communicating	
Power Module Cooling Device 1	Communicating	

The **MM Built-in Self Test (BIST) Results** section displays BIST results for the management modules. The test results for both the primary and standby management modules are kept updated. The **Last Update** field shows when the test results for each management module were collected.

MM BIST Results

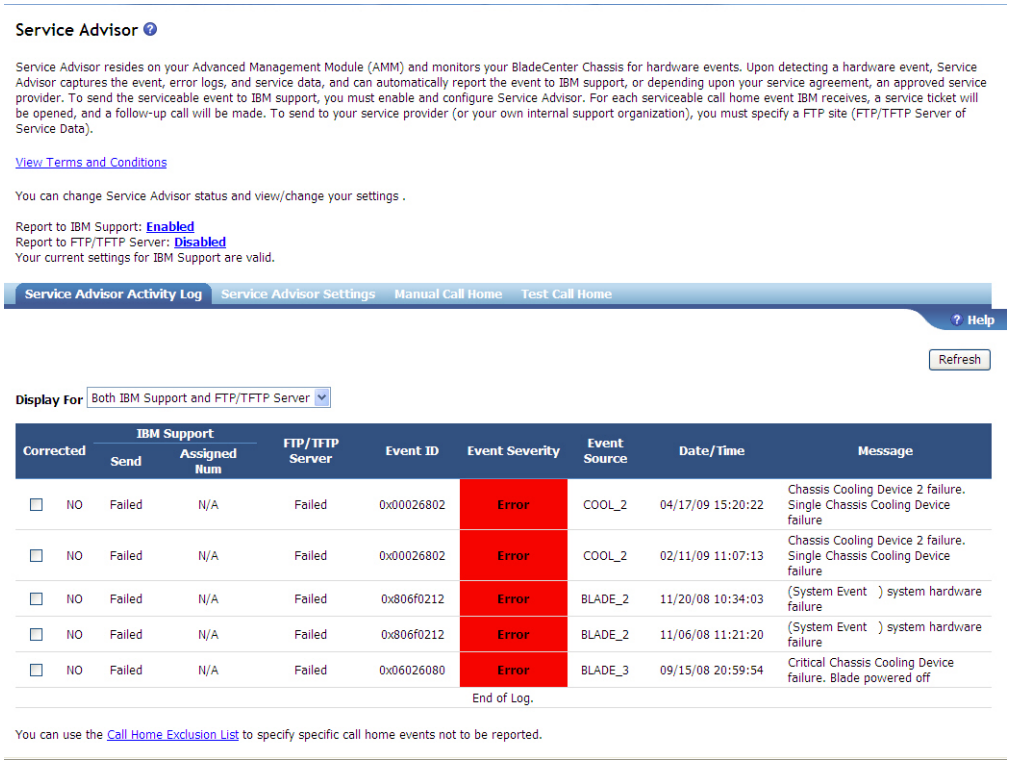
Status:
Last update: 6/01/2009 15:37

Function	MM Bay 1 (Primary)	MM Bay 2 (Empty)
Blade Management Bus 1	Passed	
Blade Management Bus 2	Passed	
Real-time Clock	Passed	
Local Management Bus	Passed	
Primary File System	Passed	
Backup File System	Passed	
Boot Loader	Passed	
Ethernet Port (eth0)	Passed	
External Management Bus	Passed	
Internal Ethernet Switch	Passed	
Video Capture	Passed	
USB Keyboard/Mouse Emulation	Passed	
USB Mass Storage Emulation	Passed	
USB Keyboard/Mouse Firmware	Passed	
USB Mass Storage Firmware	Passed	
Primary Core	Passed	
Backup Core	Passed	
Internal I/O Expander	Passed	
Remote Control Firmware	Passed	
Physical Network Link	Passed	
Logical Network Link	Passed	

Refresh

Service Advisor

Select **Service Tools → Service Advisor** to set up the BladeCenter Service Advisor to automatically send hardware and firmware serviceability information to IBM.



Note: Although Service Advisor can send alerts 24 hours a day, 7 days a week, your service provider will respond according to the arrangement that you have in place with them. Please contact them if you have any questions. For information about the terms of the warranty and getting service and assistance, see the Warranty and Support Information document for your BladeCenter device. You can obtain up-to-date information about your BladeCenter device at http://www.ibm.com/bladecenter/.

The **Service Advisor Activity Log** tab displays all events that can be reported. Click the **Call Home Exclusion List** link to select events that should not be reported (contact IBM before using this feature). The **Service Advisor Settings** tab allows you to define the service advisor contact and configuration information. The **Manual Call Home** and **Test Call Home** tabs allow you to generate test messages. The first time you configure the BladeCenter Service Advisor, or if the management module firmware was reset to the default values, you will need to view and accept a license agreement, define your contact information, and enable the service advisor feature. See “IBM Service Advisor” on page 75 for additional information and instructions.

Note: If you are using a Linux TFTP server to send hardware and firmware serviceability information to IBM, you will need to modify the TFTP configuration file. See “Configuring Linux TFTP server” on page 63.

Scalable Complex

For an advanced management module, select the choices in **Scalable Complex** to view and manage scalable complexes in the BladeCenter unit.

Note:

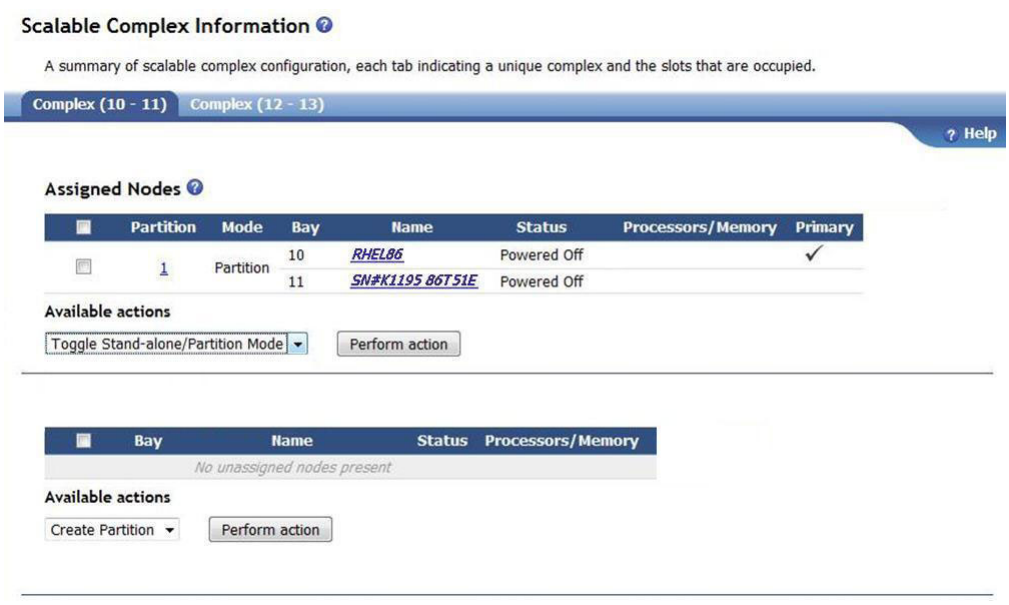
- These pages are available only when a blade server that supports scalable complexes is installed in the BladeCenter unit; if no blade servers supporting this feature are installed, the Scalable Complex section is not displayed.
- All blade servers in a scalable complex must be at the same firmware level. Coordinated update of firmware for all blade servers in a scalable complex is supported by the advanced management module (see "Firmware Update" on page 126 for additional information).

A scalable complex allows blade servers, referred to as nodes, to be placed in logical groups called partitions. Blade servers in a partition act as a single system and can share resources with each other. Single blade servers can be configured as a single node stand-alone partition so that they will retain this configuration if they are installed in another BladeCenter unit.

Configuration

Select **Scalable Complex → Configuration** to view and change blade server scalable complex settings.

The following illustration shows available actions for assigned nodes in a scalable complex. The page opens with the tab for the first scalable complex displayed. If other scalable complexes are available, you can click on each tab to view and modify information for each complex.



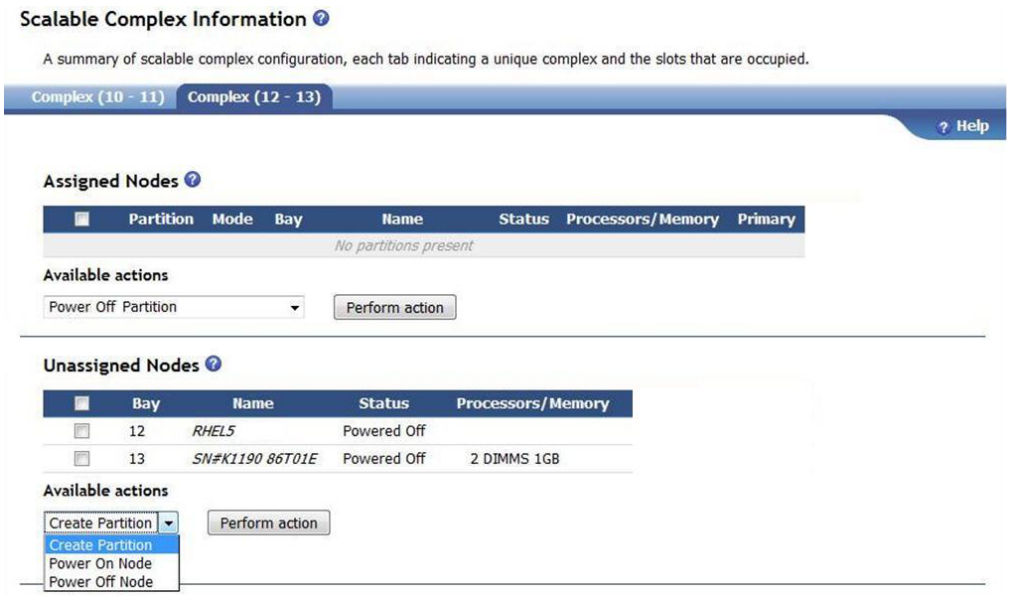
In a scalable complex, each node is a blade server. The blade server nodes can be grouped into partitions that function as a single system and share resources. The name of each node is a link to detailed information about the blade server it represents.

The following **Available actions** can be applied to a selected partition and its blade server nodes by clicking **Perform action**. Select one or more partitions in a complex using its check box.

- Power off partition.
- Power on partition.
- Power cycle partition: if the partition is off, it will turn on. If the partition is on, it will turn off and then turn on.
- Remove partition: returns all the blade server nodes in the partition to an unassigned state.
- Toggle stand-alone/partition mode: a partition set to stand-alone mode operates as a single blade server system. Single blade servers set up as a stand-alone partition will perform consistently if they are installed in another BladeCenter unit.

Note: A partition must be powered off to remove it.

The following illustration shows available actions for unassigned nodes in a scalable complex.



The following **Available actions** can be applied to a selected blade server node by clicking **Perform action**. Select one or more nodes in a complex using its check box.

- Power off node: turns the selected nodes off.
- Power on node: turns the selected nodes on.
- Cycle node: if the selected nodes are off, they will turn on. If the selected nodes are on, they will turn off and then turn on.
- Create partition: groups all the selected blade server nodes into a partition.

Note:

- To create a partition, all the nodes being grouped in it must be powered off.
- Creating a partition with blade server nodes that are enabled for the optional Blade Open Fabric Manager (BOFM) feature might cause loss of ports configured for Open Fabric Manager.

Appendix. 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.

Use this information to obtain additional information about IBM and IBM products, determine what to do if you experience a problem with your IBM system or optional device, and determine 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.

If you believe that you require IBM to perform warranty service on your IBM product, the IBM service technicians will be able to assist you more efficiently if you prepare before you call.

- 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.
- Check for updated firmware and operating-system device drivers for your IBM product. The IBM Warranty terms and conditions state that you, the owner of the IBM product, are responsible for maintaining and updating all software and firmware for the product (unless it is covered by an additional maintenance contract). Your IBM service technician will request that you upgrade your software and firmware if the problem has a documented solution within a software upgrade.
- If you have installed new hardware or software in your environment, check http://www.ibm.com/servers/eserver/serverproven/compat/us/eserver.html to make sure that the hardware and software is supported by your IBM product.
- Go to http://www.ibm.com/systems/support/ to check for information to help you solve the problem.
- Gather the following information to provide to IBM Support. This data will help IBM Support quickly provide a solution to your problem and ensure that you receive the level of service for which you might have contracted.
  - Hardware and Software Maintenance agreement contract numbers, if applicable
  - Machine type number (IBM 4-digit machine identifier)
  - Model number
  - Serial number
  - Current system UEFI and firmware levels
  - Other pertinent information such as error messages and logs
- Go to http://www.ibm.com/support/electronic/portal/ to submit an Electronic Service Request. Submitting an Electronic Service Request will start the process of determining a solution to your problem by making the pertinent information available to IBM Support quickly and efficiently. IBM service technicians can start working on your solution as soon as you have completed and submitted an Electronic Service Request.

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/.

Getting help and information from the World Wide Web

Up-to-date information about IBM products and support is available on the World Wide Web.

On the World Wide Web, up-to-date information about IBM systems, optional devices, services, and support is available at http://www.ibm.com/systems/support/. IBM System x information is at http://www.ibm.com/systems/x/ . IBM BladeCenter information is at http://www.ibm.com/systems/bladecenter. IBM IntelliStation information is at http://www.ibm.com/systems/bladecenter/ .

How to send DSA data to IBM

Use the IBM Enhanced Customer Data Repository to send diagnostic data to IBM.

Before you send diagnostic data to IBM, read http://www.ibm.com/de/support/ecurep/send_http.html .

You can use any of the following methods to send diagnostic data to IBM:

- **Standard upload:** http://www.ibm.com/de/support/ecurep/send_http.html
- **Standard upload with the system serial number:** http://www.ecurep.ibm.com/app/upload_hw/
- **Secure upload:** http://www.ibm.com/de/support/ecurep/send_http.html#secure
- **Secure upload with the system serial number:** https://www.ecurep.ibm.com/app/upload_hw/

Software service and support

Through IBM Support Line, you can get telephone assistance, for a fee, with usage, configuration, and software problems with your IBM products.

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/us/index.wss 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 Business Partners** 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

Use this information to contact 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

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 websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product, and use of those websites 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 are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies.

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 and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

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.

Important notes

Processor speed indicates 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 that are available from IBM.

Maximum memory might 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 might differ from its retail version (if available) and might not include user manuals or all program functionality.

Particulate contamination

Attention: Airborne particulates (including metal flakes or particles) and reactive gases acting alone or in combination with other environmental factors such as humidity or temperature might pose a risk to the device that is described in this document.

Risks that are posed by the presence of excessive particulate levels or concentrations of harmful gases include damage that might cause the device to malfunction or cease functioning altogether. This specification sets forth limits for particulates and gases that are intended to avoid such damage. The limits must not be viewed or used as definitive limits, because numerous other factors, such as temperature or moisture content of the air, can influence the impact of particulates or environmental corrosives and gaseous contaminant transfer. In the absence of specific limits that are set forth in this document, you must implement practices that maintain particulate and gas levels that are consistent with the protection of human health and safety. If IBM determines that the levels of particulates or gases in your environment have caused damage to the device, IBM may condition provision of repair or replacement of devices or parts on implementation of appropriate remedial measures to mitigate such environmental contamination. Implementation of such remedial measures is a customer responsibility.

Table 6. Limits for particulates and gases

Contaminant	Limits
Particulate	• The room air must be continuously filtered with 40% atmospheric dust spot efficiency (MERV 9) according to ASHRAE Standard 52.2[1]. • Air that enters a data center must be filtered to 99.97% efficiency or greater, using high-efficiency particulate air (HEPA) filters that meet MIL-STD-282. • The deliquescent relative humidity of the particulate contamination must be more than 60%[2]. • The room must be free of conductive contamination such as zinc whiskers.
Gaseous	• Copper: Class G1 as per ANSI/ISA 71.04-1985[3] • Silver: Corrosion rate of less than 300 Å in 30 days

1. ASHRAE 52.2-2008 - Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.
2. The deliquescent relative humidity of particulate contamination is the relative humidity at which the dust absorbs enough water to become wet and promote ionic conduction.
3. ANSI/ISA-71.04-1985. Environmental conditions for process measurement and control systems: Airborne contaminants. Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.

Documentation format

The publications for this product are in Adobe Portable Document Format (PDF) and should be compliant with accessibility standards. If you experience difficulties when you use the PDF files and want to request a web-based format or accessible PDF document for a publication, direct your mail to the following address:

Information Development
IBM Corporation
205/A015

3039 E. Cornwallis Road
P.O. Box 12195
Research Triangle Park, North Carolina 27709-2195
U.S.A.

In the request, be sure to include the publication part number and title.

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Telecommunication regulatory statement

This product is not intended to be connected directly or indirectly by any means whatsoever to interfaces of public telecommunications networks, nor is it intended to be used in a public services network.

Electronic emission notices

When you attach a monitor to the equipment, you must use the designated monitor cable and any interference suppression devices that are supplied with the monitor.

Federal Communications Commission (FCC) statement

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

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

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

Industry Canada Class A emission compliance statement

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

Avis de conformité à la réglementation d'Industrie Canada

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

Australia and New Zealand Class A statement

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

European Union EMC Directive conformance statement

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a nonrecommended modification of the product, including the fitting of non-IBM option cards.

Attention: This is an EN 55022 Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Responsible manufacturer:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
914-499-1900

European Community contact:

IBM Technical Regulations, Department M456
IBM-Allee 1, 71137 Ehningen, Germany
Telephone: +49 7032 15-2937
Email: tjahn@de.ibm.com

Germany Class A statement

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der IBM gesteckt/eingebaut werden.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden: “Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen.”

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem “Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)”. Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:

IBM Deutschland
Technical Regulations, Department M456
IBM-Allee 1, 71137 Ehningen, Germany
Telephone: +49 7032 15-2937
Email: tjahn@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

Japan VCCI Class A statement

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

This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI). If this equipment is used in a domestic environment, radio interference may occur, in which case the user may be required to take corrective actions.

Korea Communications Commission (KCC) statement

This is electromagnetic wave compatibility equipment for business (Type A). Sellers and users need to pay attention to it. This is for any areas other than home.

Russia Electromagnetic Interference (EMI) Class A statement

ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать радиопомехи, для снижения которых необходимы дополнительные меры

People's Republic of China Class A electronic emission statement

中华人民共和国“A类”警告声明

声 明

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

Taiwan Class A compliance statement

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

Index

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Part Number: 00D3237

Printed in USA

(1P) P/N: 00D3237