Intel® Server Blade Chassis Enterprise Management Module 2: Installation and User's Guide

A Guide for Technically Qualified Assemblers of Intel® Identified Subassemblies and Products

Intel Order Number D59324-003

Disclaimer

Information in this document is provided in connection with Intel® products. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel's Terms and Conditions of Sale for such products, Intel assumes no liability whatsoever, and Intel disclaims any express or implied warranty, relating to sale and/or use of Intel products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Intel products are not designed, intended or authorized for use in any medical, life saving, or life sustaining applications or for any other application in which the failure of the Intel product could create a situation where personal injury or death may occur. Intel may make changes to specifications and product descriptions at any time, without notice.

Intel products are not designed, intended or authorized for use in any medical, life saving, or life sustaining applications, or for any other application in which the failure of the Intel product could create a situation where personal injury or death may occur. Intel may make changes to specifications and products descriptions at any time, without notice.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)

This product includes software developed by the OpenSSL Project for use in the Open SSL Toolkit. (http://www.openssl.org/).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

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

* Other names and brands may be claimed as the property of others.

Safety and Regulatory Information

Note: *The service procedures are designed to help you isolate problems. They are written with the assumption that you have model-specific training on all computers, or that you are familiar with the computers, functions, terminology, and service information provided in this manual.*

General Safety

Follow these rules to ensure general safety:

- Observe good housekeeping in the area of the machines during and after maintenance.
- When lifting any heavy object:
  - — Ensure you can stand safely without slipping.
  - — Distribute the weight of the object equally between your feet.
  - — Use a slow lifting force. Never move suddenly, or twist, when you attempt to lift.
  - — Lift by standing or by pushing up with you leg muscles; this action removes the strain from the muscles in your back. Do not attempt to lift any object that weighs more than 16 kg (35lb) or any object that you think is too heavy for you.
- Do not perform any action that causes hazards to the customer, or makes the equipment unsafe.
- Before you start the machine, ensure that other service representatives and the customer's personnel are not in a hazardous position.
- Place removed covers and other parts in a safe place, away from all personnel, while you are servicing the machine.
- Keep your tool case away from walk areas so that other people will not trip over it.
- Do not wear loose clothing that can be trapped in the moving parts of a machine. Ensure that your sleeves are fastened or rolled up above your elbows. If your hair is long, fasten it.
- Insert the ends of your necktie or scarf inside clothing, or fasten it with a non-conducting clip, approximately 8 centimeters (3 inches) from the end.
- Do not wear jewelry, chains, metal-frame eyeglasses, or metal fasteners for your clothing.

  Remember: Metal objects are good electrical conductors.
- Wear safety glasses when you are: hammering, drilling soldering, cutting wire, attaching springs, using solvents, or working in any other conditions that might be hazardous to your eyes.

- After service, reinstall all safety shields, guards, labels, and ground wires. Replace any safety device that is worn or defective.
- Reinstall all covers correctly before returning the machine to the customer.

Electrical Safety

Caution: *Electrical current from power, telephone, and communication cables can be hazardous. To avoid personal injury or equipment damage, disconnect the server system power cords, telecommunication systems, networks, and modems before you open the server covers, unless instructed otherwise in the installation and configuration procedures.*

Caution: *Lithium Battery Replacement: Replace with the same or equivalent battery type as recommended by manufacturer.*

Do not:

- *Throw or immerse into water*
- *Heat to more than 100ºC (212ºF)*
- *Repair or disassemble*

Important: *Disconnect all power before performing a mechanical inspection.*

Observe the following rules when working on electrical equipment.

- Use only approved tools and test equipment. Some hand tools have handles covered with a soft material that does not protect you when working with live electrical currents.
- Many customers have rubber floor mats (near their equipment) that contain small conductive fibers to decrease electrostatic discharges. Do not use this type of mat to protect yourself from electrical shock.
- Find the emergency power-off (EPO) switch, disconnect switch, or electrical outlet in the room. If an electrical accident occurs, you can quickly turn off the switch or unplug the power cord.
- Do not work alone under hazardous conditions, or near equipment that has hazardous voltages.
- Disconnect all power before:
  - Performing a mechanical inspection
  - Working near power supplies
  - Removing or installing main units
- Before you start to work on the machine, unplug the power cord. If you cannot unplug it, ask the customer to power-off the wall box (that supplies power to the machine) and to lock the wall box in the off position.

- If you need to work on a machine that has exposed electrical circuits, observe the following precautions:
  - Ensure that another person, familiar with the power-off controls, is near you. Remember: another person must be there to switch off the power, if necessary.
  - Use only one hand when working with powered-on electrical equipment; keep the other hand in your pocket or behind your back.
  - Remember: There must be a complete circuit to cause electrical shock. By observing the above rule, you may prevent a current from passing through your body.
- When using testers, set controls correctly and use the approved probe leads and accessories for that tester.
- Stand on suitable rubber mats (obtained locally, if necessary) to insulate you from grounds such as metal floor strips and machine frames.
- Observe the special safety precautions when you work with very high voltages; these instructions are in the safety sections of the maintenance information. Use extreme care when measuring high voltages.
- Regularly inspect and maintain your electrical hand tools for safe operational condition.
- Do not use worn or broken tools and testers.
- Never assume that power has been disconnected from a circuit. First, check that it has been powered-off.
- Always look carefully for possible hazards in your work area. Examples of these hazards are moist floors, non-guaranteed power extension cables, power surges, and missing safety grounds.
- Do not touch live electrical circuits with the reflective surface of a plastic dental inspection mirror. The surface is conductive; such touching can cause personal injury and machine damage.
- When the power is on and power supply units, blowers and fans are removed from their normal operating position in a machine, do not attempt to service the units. This practice ensures correct grounding of the units.
- If an electrical accident occurs, use caution:
  - Switch power off
  - Send another person to get help/medical aid

Handling Electrostatic Discharge-sensitive Devices

Any computer part containing transistors or integrated circuits (IC) should be considered sensitive to electrostatic discharge (ESD). ESD damage can occur when there is a difference in charge between objects. Protect against ESD damage by equalizing the charge so that the server, the part, the work mat, and the person handling the part are all at the same charge.

Note: *Use product-specific ESD procedures when they exceed the requirements noted here.*

Make sure that the ESD-protective devices you use have been certified (ISO 9000) as fully effective.

When handling ESD-sensitive parts:

- Keep the parts in protective packages until they are inserted into the product.
- Avoid contact with other people.
- Wear a grounded wrist strap against your skin to eliminate static on your body.
- Prevent the part from touching your clothing. Most clothing is insulative and retains a charge even when you are wearing a wrist strap.
- Use the black side of a grounded work mat to provide a static-free work surface. The mat is especially useful when handling ESD-sensitive devices.
- Select a grounding system, such as those in the following list, to provide protection that meets the specific service requirement.
  - — Attach the ESD ground clip to any frame ground, ground braid, or green-wire ground.
  - — Use an ESD common ground or reference point when working on a double-insulated or battery-operated system. You can use coax or connector-outside shells on these systems.
  - — Use the round ground-prong of the AC plug on AC-operated computers.

Note: *The use of a grounding system is desirable but not required to protect against ESD damage.*

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

To avoid a shock hazard:

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

Connect and disconnect cables as described in the following table when installing, moving, or opening covers on this product or attached devices.

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

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

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

Regulatory Specifications and Disclaimers

Safety Compliance

USA	UL 60950-1 / CAN / CSA C22.2 No. 60950-1-03
Canada	cUL certified / CSA 22.2. No. 60950-1-03 for Canada (product bears the single cUL mark for U.S. and Canada)
Europe	Low Voltage Directive, 73/23/EEC UL/CB to EN60950-1 (2001)
International	UL/CB to IEC 60950-1 (2001) UL/CB - 60950-1 (2001) UL/CB - EMKO-TSE (74-SEC) 207/94
Australia/New Zealand	CB Report to IEC 60950-1 (2001) plus international deviations

Electromagnetic Compatibility (EMC)

USA	FCC CFR 47 Part 2 and 15, Verified Class A Limit
Canada	IC ICES-003 Class A Limit
Europe	EMC Directive, 89/336/EEC EN55022, Class A Limit, Radiated & Conducted Emissions EN55024 ITE Specific Immunity Standard EN61000-4-2 ESD Immunity (Level 2 Contact Discharge, Level 3 Air Discharge) EN61000-4-3 Radiated Immunity (Level 2) EN61000-4-4 Electrical Fast Transient (Level 2) EN61000-4-5 AC Surge EN61000-4-6 Conducted RF EN61000-4-8 Power Frequency Magnetic Fields EN61000-4-11 Voltage Dips and Interrupts
Japan	VCCI Class A ITE (CISPR 22, Class A Limit)
Australia/New Zealand	AS/NZS 3548, Class A Limit
Korea	RRL Approval
Russia	GOST Approval
International:	CISPR 22, Class A Limit

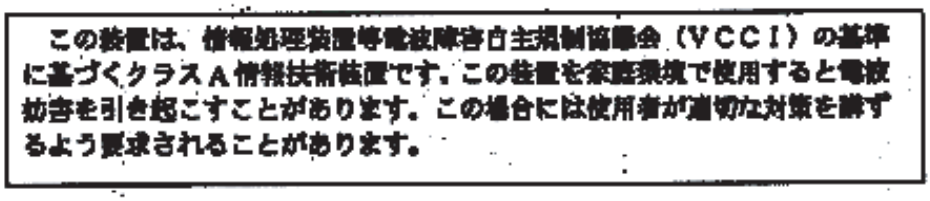
Electromagnetic Compatibility Notice (USA)

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.

Electromagnetic Compatibility Notices (International)

Europe (CE Declaration of Conformity): This product has been tested in accordance to, and complies with the Low Voltage Directive (73/23/EEC) and EMC Directive (89/336/EEC). The product has been marked with the CE Mark to illustrate its compliance.

Japan EMC Compatibility:

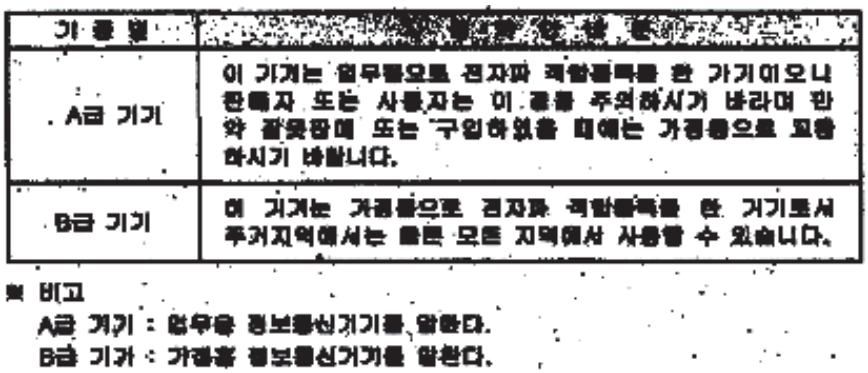


English translation of the notice above: This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

ICES-003 (Canada): Cet appareil numérique respecte les limites bruits radioélectriques applicables aux appareils numériques de Classe A prescrites dans la norme sur le matériel brouilleur: “Appareils Numériques”, NBM-003 édictée par le Ministre Canadian des Communications.

English translation of the notice above: This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the interference-causing equipment standard entitled “Digital Apparatus”, ICES-003 of the Canadian Department of Communications.

RRL Korea:



기 종 별	
A급 기기	이 기기는 업무용으로 전자파 적합등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며 만약 잘못팔았을 때 또는 구입하였을 때에는 가정용으로 교환하시기 바랍니다.
B급 기기	이 기기는 가정용으로 전자파 적합등록을 한 기기로서 주거지역에서는 물론 모든 지역에서 사용할 수 있습니다.

※ 비고
A급 기기 : 업무용 정보통신기기를 말한다.
B급 기기 : 가정용 정보통신기기를 말한다.

English translation of the previous notice:

Device	User's Information
Class A device	This device complies with RRL EMC and is operated in commercial environment so that distributors or users pay attention to this point. If the product is sold or purchased improperly, please exchange this product to what can be used at home.
Class B device	This device complies with RRL EMC and is operated in a residential area so that it can be used at all other location as well as residential area.
Remarks: Class A device - operated in a commercial area. Class B device - operated in a residential area.	

Contents

1 Introduction

This *Installation and User's Guide* contains information about installing and configuring your Intel® Server Blade Chassis Enterprise Management Module 2 and managing components that are installed in an Intel® Blade Server Chassis Enterprise SBCE. You configure Blade Server Chassis Enterprise SBCE components using the Management Module 2 to set information such as IP addresses.

Note: *In the remainder of this document the Intel® Server Blade Chassis Enterprise Management Module 2 might be referred to as either the Management Module 2 or the SBCECMM2.*

This guide is for customers of the Intel® Blade Server Chassis Enterprise SBCE that are configured with the next generation chassis Intel® Server Blade Chassis Enterprise Management Module 2.

The Management Module 2 provides system-management functions and keyboard/video/mouse (KVM) multiplexing for all the blade servers in the Blade Server Chassis Enterprise SBCE that support KVM. It controls a serial port for remote connection; the external keyboard, mouse, and video connections for use by a local console; and a 10/100 Mbps Ethernet remote-management connection.

The Blade Server Chassis Enterprise SBCE comes with one hot-swap Management Module 2 in management module bay 1. You can add an additional Management Module 2 in management module bay 2. Only one of the Management Module 2 units can be active at any one time, functioning as the primary management module. A second Management Module 2 unit, if installed, provides redundancy. It remains inactive until you switch it to act as the primary management module.

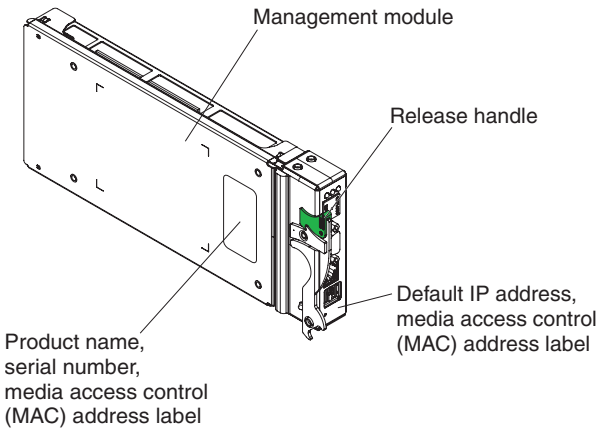
If two Management Module 2 units are installed in a Blade Server Chassis Enterprise SBCE, both must always have the same level of firmware and the same IP address. The firmware must support redundant management module function, to ensure changeover of control from the primary (active) management module to the redundant management module. The latest level of management module firmware is available at http://support.intel.com/support/motherboards/server/blade.htm.

The Management Module 2 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 Blade Server Chassis Enterprise SBCE shared media tray (removable-media drives and USB connector).

Record information about the Management Module 2 in the following table.

Product name	Intel® Server Blade Chassis Enterprise Management Module 2
Serial number	
Media access control (MAC) address	

The product name, serial number, and media access control (MAC) address are located on the identification label on the side of the Management Module 2. The MAC address and along the default IP address are on a separate label on the bottom of the front of the Management Module 2.



Note: *The sample screens and hardware that appear in this document might differ slightly from the screens and hardware you have.*

Related Documentation

In addition to this *Installation Guide and User's Guide*, you may need to refer to the following documents. These documents are provided with your Intel® Server Blade Chassis Enterprise Management Module 2. The latest versions of all Blade Server Chassis Enterprise SBCE documentation are at http://support.intel.com/support/motherboards/server/blade.htm.

- *Intel® Server Boards and Server Chassis Safety Information*

  This multi-lingual publication contains safety information, cautions, and warning statements. It is rovided in a PDF file on the Management Module 2 *Resource CD*.

- *Intel® Blade Server Chassis Enterprise SBCE: Installation and User's Guide*

  This document provides general configuration information about your server chassis, including information about features, how to configure your server, and how to get help.

- *Intel® Blade Server Chassis Enterprise SBCE Rack Installation Instructions*

  This document tells you hot to install your *Intel®* Blade Server Chassis Enterprise SBCE into a rack.

- *Intel® Blade Server Chassis Enterprise SBCE: Hardware Maintenance Manual and Troubleshooting Guide.*

  This document provides information to help you solve problems yourself and it provides information that is helpful for service technicians.

- *Intel® Blade Server Chassis Enterprise Chassis Management Module: Installation and User's Guide*

  This document provides general configuration information about your chassis management module, including information about features, how to configure it, and how to get help

Depending on your blade server model, additional publications might also be included on your *Resource CD*.

Notices and Statements in this 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 could occur.*

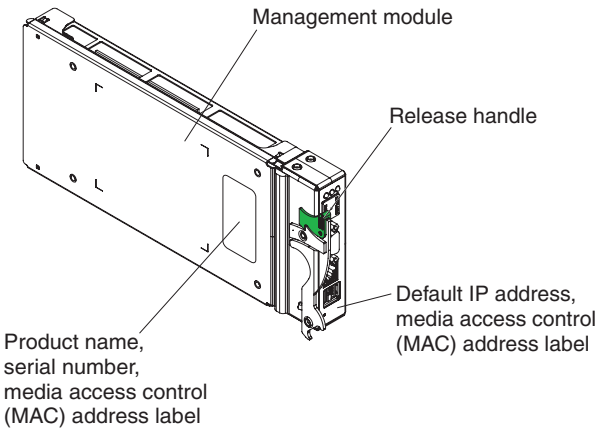
Caution: *These statements indicate situations that can be potentially hazardous to you. A caution statement is placed just before the description of a potentially hazardous procedure step or situation.*

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.*

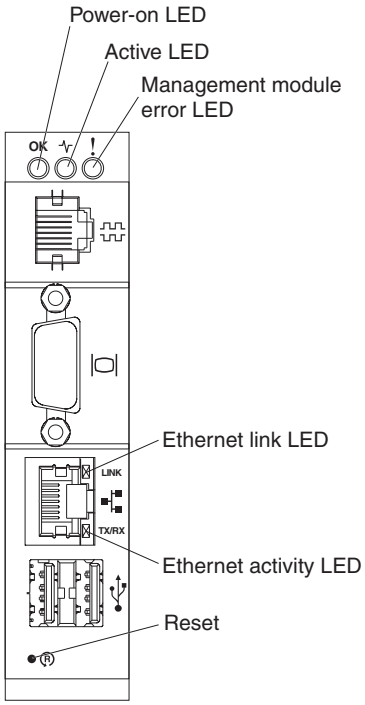
2 Overview of the Intel® Server Blade Chassis Enterprise Management Module 2

This chapter describes the indicators, controls, and external connectors on the Intel® Server Blade Chassis Enterprise Management Module 2. See the documentation that comes with each management module for a description of the LEDs on the module.

The following illustration shows the Management Module 2.



Management Module Indicators and Controls

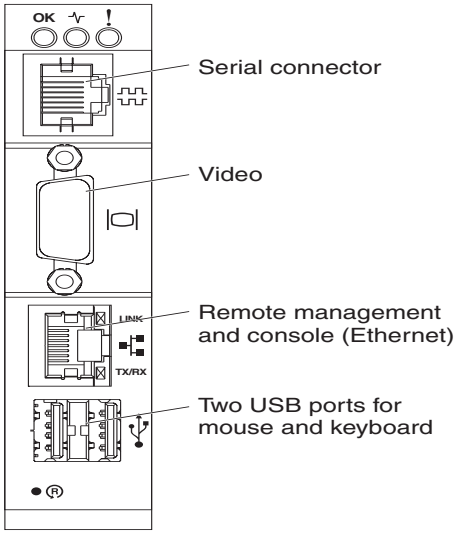


The following management module LEDs provide status information about the Management Module 2 and remote-management connection.

- **Power-on LED**: When this green LED is lit, it indicates that the Management Module 2 has power.
- **Active LED**: When this green LED is lit, it indicates that the Management Module 2 is actively controlling the Blade Server Chassis Enterprise SBCE. Only one Management Module 2 unit actively controls the Blade Server Chassis Enterprise SBCE. If two management modules are installed in the Blade Server Chassis Enterprise SBCE, this LED is lit on only one module.
- **Management module error LED**: When this amber LED is lit, it indicates that an error has been detected in the Management Module 2. When this LED is lit, the Blade Server Chassis Enterprise SBCE system error LED is also lit.
- **Ethernet Link LED**: When this green LED is lit, there is an active connection through the port to the network.
- **Ethernet activity LED**: When this green LED is flashing, it indicates that there is activity through the port over the network link.
- **Reset button**: When you press this button the blowers operate at full speed while the Management Module 2 is initializing.
  - — Press and release the reset button to restart the Management Module 2.
  - — Press and hold the reset button for 8 seconds to restore the Management Module 2 to the factory default settings.

Management Module Input and Output Connectors

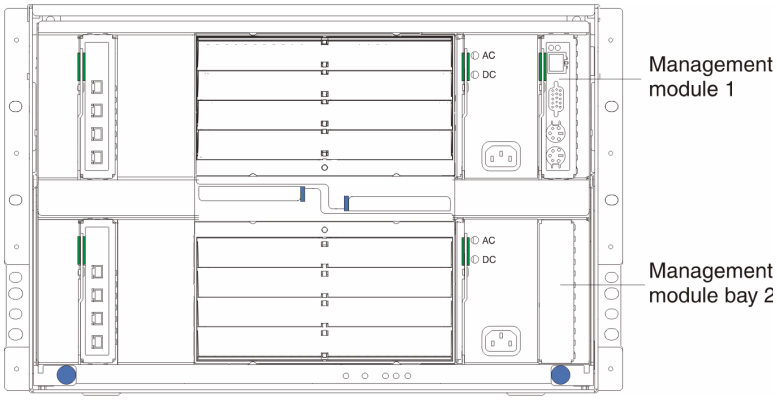
The Management Module 2 has a serial connector, a video connector, a remote management and console connector, and two USB connectors for keyboard and mouse.



- **Serial connector**: Use this connection to configure and manage the Blade Server Chassis Enterprise SBCE components over a serial line through the management module command-line interface (CLI). This connector provides local access to the CLI and redirection to the Serial over LAN (SOL) interface of any processor blade server. For example, you can connect a notebook computer to the serial connector and use a terminal emulator program to configure the IP addresses, user accounts, and other management settings through the CLI user interface. See the *Intel® Blade Server Chassis Enterprise SBCE*: *Command-Line Interface Reference Guide* and the *Intel® Blade Server Chassis Enterprise SBCE: Serial Over LAN (SOL) Setup Guide* for more information.
- **Video connector**: Use this connector to connect a compatible SVGA or VGA video monitor to the Blade Server Chassis Enterprise SBCE.
- **Remote management and console (Ethernet) connector**: Use this connector for an Ethernet remote connection to a network-management station on the network. See "Configuring the Management Module for Remote Access" on page 29 for more information about remote configuration.
- **Two USB ports for mouse and keyboard**: Use these two connectors for local mouse and keyboard connectivity. The blade servers share the management module USB ports through the Blade Server Chassis Enterprise SBCE KVM interface. The KVM interface has ownership of these ports.

3 Installing an Intel® Server Blade Chassis Enterprise Management Module 2

The following illustration shows the management module bay locations.



Attention: *To maintain proper system cooling, each module bay must contain either a module or a filler module; each blade bay must contain either a blade or a filler blade.*

Installation Guidelines

Before you install the Intel® Server Blade Chassis Enterprise Management Module 2, read the following information:

- Read "Safety and Regulatory Information" on page iii and read the safety statements in the Blade Server Chassis Enterprise SBCE documentation.
- The green color on components and labels in your Blade Server Chassis Enterprise SBCE identifies hot-swap components. You can install or remove hot-swap modules and, with some restrictions, hot-swap blade servers while the Blade Server Chassis Enterprise SBCE is running. For details about installing or removing a Management Module 2, see the detailed information in this chapter.
- For a list of supported options for your Blade Server Chassis Enterprise SBCE, see http://support.intel.com/support/motherboards/server/blade.htm.

You do not need to disconnect the power from your Blade Server Chassis Enterprise SBCE to replace any of the hot-swap modules on the rear of the chassis. You must shut down the operating system and turn off a hot-swap blade server on the front of the chassis before removing the blade server, but you do not need to shut down the chassis itself.

System Reliability Guidelines

To help ensure proper Blade Server Chassis Enterprise SBCE cooling and system reliability, make sure that the following requirements are met:

- Each of the module bays on the front and rear of the Blade Server Chassis Enterprise SBCE has either a module or a module filler installed.
- Each of the blade server bays on the front of the Blade Server Chassis Enterprise SBCE has either a blade server or a blade filler installed.
- Each of the drive bays in a blade-server storage expansion option has either a hot-swap drive or a panel filler installed.
- A removed hot-swap module, blade server, or drive is be replaced within 1 minute of removal.
- Cables for optional modules are routed according to the documents that come with the modules.
- A failed blower is replaced as soon as possible, to restore cooling redundancy.

Failure to replace a blade server or module with another blade server, module, blade filler, or module filler within 1 minute can affect the system performance of the blade servers.

Handling Static-sensitive Devices

Attention: *Static electricity can damage the* Blade Server Chassis Enterprise SBCE *system and other electronic devices. To avoid damage, keep static-sensitive devices in their static-protective packages until you are ready to install them.*

To reduce the possibility of electrostatic discharge (ESD), observe the following precautions:

- See the *Installation and User's Guide* that comes with your Blade Server Chassis Enterprise SBCE to locate the ESD connector. Not all Blade Server Chassis Enterprise SBCEs have a ESD connector.
- Limit your movement. Movement can cause static electricity to build up around you.
- Handle the device carefully, holding it by its edges or its frame.
- Do not touch solder joints, pins, or exposed printed circuitry.
- Do not leave the device where others can handle and damage it.
- While the device is still in its static-protective package, touch it to an unpainted metal part of the Blade Server Chassis Enterprise SBCE or any unpainted surface on any other grounded rack component for at least 2 seconds. This drains static electricity from the package and from your body.
- Remove the device from its package and install it immediately without setting down the device. If it is necessary to set down the device, put it back into its static-protective package.
- Take additional care when handling devices during cold weather. Heating reduces indoor humidity and increases static electricity.

Hardware and Software Requirements

The Management Module 2 supports the following Web browsers for remote (client) access. The client Web browser must be Java*-enabled, must support JavaScript* 1.2 or later, and must have the Java Virtual Machine (JVM) version 1.4.2-08 or later (but earlier than 1.5) Plug-in installed. The JVM Plug-in is available from http://www.java.com/.

- Microsoft Internet Explorer* 5.5 or later (with latest Service Pack installed)
- Netscape Navigator* 7.0 or later
- Mozilla* version 1.3 or later

Note: *The Remote Disk feature works only with the Microsoft Windows 2000 operating system or later.*

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

- Microsoft Windows Server 2003*
- Microsoft Windows 2000* with Service Pack 4 or later
- Red Hat* Linux version 7.3
- SUSE* Linux version 8.0
- Novell NetWare* 6.5

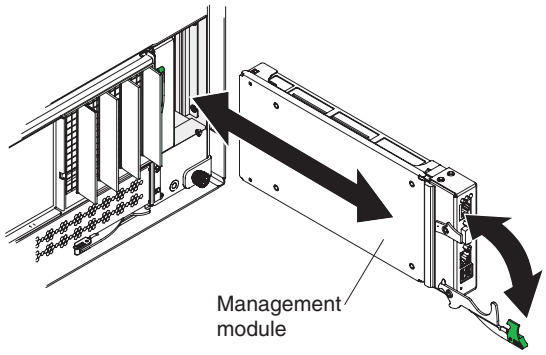
The management module Web interface does not support double-byte character set (DBCS) languages.

Installing a Management Module 2

The following illustration shows how to install a Management Module 2 in an Intel® Blade Server Chassis Enterprise SBCE. Your Blade Server Chassis Enterprise SBCE might differ from the illustrations in this document.

When you install a Management Module 2, if the Blade Server Chassis Enterprise SBCE is not connected to a DHCP server on the network, it takes up to 3 minutes for the Management Module 2 to use the default (static) IP address.

Attention: *To maintain proper system cooling, each module bay must contain either a module or a module filler.*



Note:

- *If you replace a redundant Management Module 2, you must install the same type of management module as the primary management module.*
- *These instructions assume that the Blade Server Chassis Enterprise SBCE is connected to a power supply.*
- *After failover, you might not be able to establish a network connection to the Management Module 2 for 5 minutes. This is because the network might include switches, routers, and hubs that might not allow (or relay) an address resolution protocol (ARP) from the new Management Module 2 to update the network cached ARP table. Without this information relay, the new MAC address/IP association will not recognize the Management Module 2. This condition will correct itself after the ARP table times out. To prevent this condition, reconfigure the network routing setup tables to enable ARPs to be relayed from the Management Module 2.*

To install a Management Module 2, complete the following steps:

1. Read "Safety and Regulatory Information" on page iii, "Installation Guidelines" on page 9, and "Handling Static-sensitive Devices" on page 10.
2. If you are installing a secondary Management Module 2, read "Preparing for Management Module Redundancy" on page 15.
3. Remove any external devices that are blocking access to the rear of the Blade Server Chassis Enterprise SBCE. See the *Installation and User's Guide* for your Blade Server Chassis Enterprise SBCE for instructions.

4. If you are replacing the only Management Module 2 in the Blade Server Chassis Enterprise SBCE, and the Management Module 2 is functional, save the configuration file before you proceed. To save the configuration file and restore it to the replacement Management Module 2, see the *Intel® Blade Server Chassis Enterprise SBCE: Management Module Command-line Interface Reference Guide* for instructions.
5. If you are replacing a Management Module 2, remove the current module from the bay (see "Removing a Management Module 2" on page 14). If you are adding a new Management Module 2, remove the module filler from the selected management module bay and store the module filler for future use.
6. If you have not already done so, touch the static-protective package that contains the replacement Management Module 2 to an unpainted metal part of the Blade Server Chassis Enterprise SBCE or any unpainted surface on any other grounded rack component for at least 2 seconds.
7. Remove the Management Module 2 from its static-protective package.
8. Make sure that the release handle on the Management Module 2 is in the open position (perpendicular to the module).
9. Slide the Management Module 2 into the selected management module bay until it stops.
10. Push the release handle on the front of the Management Module 2 to the closed position.
11. Make sure that the power-on LED on the Management Module 2 is lit. This indicates that the management module is operating correctly. See "Management Module Indicators and Controls" on page 6 to locate the LED.
12. Connect the cables to the Management Module 2. See "Management Module Video Settings" on page 16 for more information.
13. Replace any external components that you removed.
14. If this is the only management module in the Blade Server Chassis Enterprise SBCE, configure the new Management Module 2. See "Configuring the Management Module" on page 28 for more information.

    If this is a redundant management module, and you followed the instructions in "Preparing for Management Module Redundancy" on page 15, no configuration is necessary.

The second management module receives the configuration and status information automatically from the primary management module when necessary. The transfer of information to the redundant management module can take up to 45 minutes after it is installed.

Removing a Management Module 2

Note:

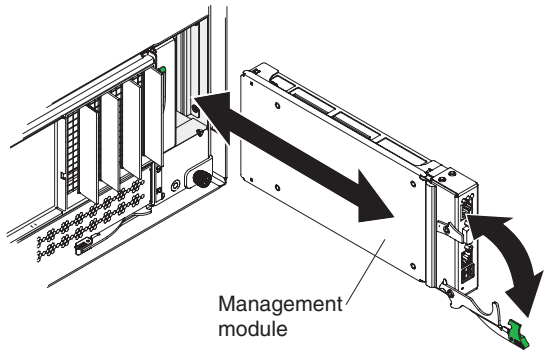
- *These instructions assume that the Blade Server Chassis Enterprise SBCE is connected to a power supply.*
- *If you are removing the active management module from the Blade Server Chassis Enterprise SBCE, stop all management module local and remote sessions before you proceed, to avoid an unexpected termination of sessions.*
- *If you are replacing the only management module in the Blade Server Chassis Enterprise SBCE and the Management Module 2 is functioning, save the configuration file before you proceed. To do so:*
  - *Under the **MM Control** section of the navigation pane, click **Configuration File**.*
  - *Follow the instructions under **Save MM Configuration**.*

  You will be able to restore the saved configuration file to the replacement Management Module 2. See "Restoring and Modifying your Management Module Configuration" on page 63 for information about applying a saved configuration file.
- *If you have just installed a second Management Module 2 in the Blade Server Chassis Enterprise SBCE, wait 45 minutes before removing the first (primary) management module. The second (redundant) management module needs this time to receive initial status information and firmware from the primary management module.*

To remove a Management Module 2, complete the following steps:

1. Read "Safety and Regulatory Information" on page iii, "Installation Guidelines" on page 9, and "Handling Static-sensitive Devices" on page 10.
2. Remove any external devices that block access to the rear of the Blade Server Chassis Enterprise SBCE. See the *Installation and User's Guide* for your Blade Server Chassis Enterprise SBCE for instructions.
3. Disconnect any cables from the Management Module 2.

4. Pull the release handle all the way toward the bottom of the Management Module 2 until it stops, as shown in the illustration. The module moves out of the bay approximately 0.6 cm (0.25 inch).



5. Slide the module out of the bay and set it aside. Within 1 minute, place either another module of the same type or a module filler in the bay.

Preparing for Management Module Redundancy

Management Module 2 redundancy requires specific minimum levels of firmware. If you install a second Management Module 2, make sure you have downloaded and applied the latest level of firmware.

To prepare your management modules for redundancy, complete the following steps:

1. Obtain the latest hardware updates from your Intel Support Representative.
2. Download the latest Management Module 2 firmware.
3. Use the Management Module 2 Web interface to apply the latest firmware to your current Management Module 2. See "Using the Management Module Web Interface" on page 23 for instructions on logging in to the Web interface.

   Note: *See the Intel® Blade Server Chassis Enterprise SBCE User's Guide for firmware update procedures. In brief:*

   - ✧ *In the MM Control section of the navigation pane, click Firmware Update.*
   - ✧ *Click Browse to locate the firmware file that you downloaded.*
   - ✧ *Click Update.*
   - ✧ *Follow the on-screen instructions.*

4. Install the second Management Module 2 in the available management module bay. For instructions, see "Installing a Management Module 2" on page 12.
5. Wait 45 minutes while the primary Management Module 2 transfers firmware and configuration information to the second management module.

The management modules are now prepared for redundancy.

Note: *Whenever power is restored to a Blade Server Chassis Enterprise SBCE that has two functional management modules, the Management Module 2 in bay 1 is, by default, the active management module, even if the module in bay 2 was the active module before power was removed.*

Management Module Video Settings

The following table lists the video resolution and refresh-rate combinations for KVM-equipped blade servers that are supported for all system configurations.

Table 1. Compliant Video Settings

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

Cabling the KVM

See “Management Module Indicators and Controls” on page 6 for the location of each connector.

If you always use a remote session to communicate with the blade servers in the Blade Server Chassis Enterprise SBCE, you do not have to connect a local KVM to the Management Module 2.

To cable the KVM for the Management Module 2, use one of the following cabling methods:

- **Keyboard and mouse with USB ports** - Connect a USB keyboard and USB mouse to the USB connector on the Management Module 2.
- **Video port** - Connect the video cable to the video connector on the Management Module 2.
- **Cable only to the active** Management Module 2 - When management module data transfer occurs, you can move the keyboard, video, and mouse cables to the active management module.
- **Use a duplicate keyboard, monitor, and mouse for the second management module -** With a second keyboard, monitor, and mouse always connected to the second management module, no switching or recabling is required when data transfer occurs.

Connecting the Management Module 2 to the Network

The Management Module 2 supports network connection through the remote management and console (Ethernet) connector or a CLI-only connection through the serial connector. You can manage the Blade Server Chassis Enterprise SBCE through the graphical-user interface that is provided by the management module Web interface or through the CLI that you access through a terminal emulator program, a Secure Shell (SSH) server, or the serial connector.

All management module network connections to blade servers that do not support KVM are made through the CLI. You can perform initial configuration of the Management Module 2 after you connect it to your network; however, because some requirements are imposed by the default management module settings, it might be easier to perform these setup operations through a temporary connection.

You can access the management module Web interface through a network or through a computer that is connected directly to the Management Module 2. To connect to the management module Web interface, you need the following equipment and information:

- A computer with Internet browser capability. To facilitate connections at multiple locations, you can use a notebook computer.
- The management module MAC address (listed on the label on the Management Module 2).
- For a networked connection to the Management Module 2, 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 need an Ethernet cable.

Network connections through the serial connector can access only the management module CLI. See the *Intel*® Blade Server Chassis Enterprise SBCE*: Management Module Command-line Interface Reference Guide* for information about accessing the management module CLI.

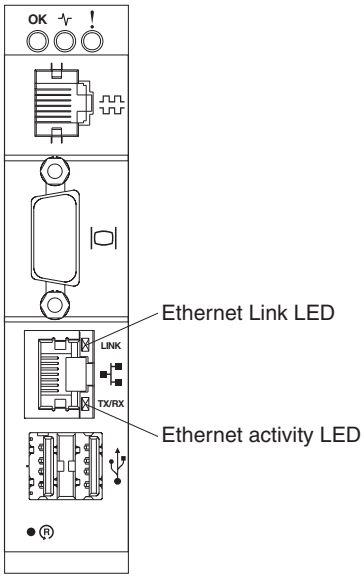
The following sections describe how to make typical network connections for a Management Module 2.

Networked Connection

To connect the Ethernet cable to the Management Module 2, complete the following steps:

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

The following illustration shows the locations of the Ethernet LEDs.



Direct Connection

To connect the Ethernet cable directly to the Management Module 2, complete the following steps:

1. Connect one end of a Category 5 or higher Ethernet cable to the remote management and console (Ethernet) connector on the Management Module 2.
2. Connect the other end of the Ethernet cable to the Ethernet connector on the client computer.
3. Check the Ethernet LEDs to make sure that the network connection is working.
   - When the green Ethernet LINK LED is lit, there is an active connection through the port to the network.
   - When the green Ethernet activity (TX/RX) LED is flashing, it indicates that there is activity through the port over the network link.

Serial Connection

To connect the serial cable to the Management Module 2, complete the following steps:

1. Connect one end of an RJ-45 serial cable to the serial connector on the Management Module 2.
2. Connect the other end of the serial cable to the serial connector of the client computer, such as a notebook computer.
3. Configure the serial port of the client computer to the following values:
   - Baud rate = 57600
   - Parity = none
   - Stop bits = 1

The serial cable must have the following characteristics.

RJ-45 Signal	RJ-45 Pins	RJ-45 Cable	DB9 Signal	DB9 Pins
TxD out	6	yellow	RxD in	2
RxD in	5	green	TxD out	3
RTS out	8	white	CTS in	8
CTS in	7	brown	RTS out	7
DTR out	3	black	DSR in	6
DSR in	1	blue	DTR out	4
DCD in	2	orange	DCD in	n/a
RI in	n/a	n/a	RI in	n/a
GND	4	red	GND	5

Connecting a Remote Console to the Management Module 2 for the First Time

The following sections describe how to connect a remote console to the Management Module 2 to perform initial configuration of the Blade Server Chassis Enterprise SBCE. The Management Module 2 has the following default settings:

- IP address: 192.168.70.125
- 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 2 is configured to respond to DHCP first before using its static IP address.

The client computer that you connect to the Management Module 2 must be configured to operate on the same subnet as the Management Module 2. The IP address of the Management Module 2 must also be in the same local domain as the client computer. To connect to the Management Module 2 for the first time, you must change the Internet protocol properties on the client computer.

There are two interfaces that you can use to connect to the Management Module 2 for the first time. If you are connecting to the Management Module 2 through an Ethernet connection, you can open a Web browser and use the Web-based interface, or you can use Telnet to connect to the Management Module 2 and use the CLI to configure the module. If you are connecting through a serial connection, you can use a terminal emulator to access the CLI.

Ethernet Connection (Web-based)

After you connect the Ethernet cable from the Management Module 2 to the client computer, complete the following steps:

1. Make sure that the subnet of the client computer is set to the same value as the default management module subnet (255.255.255.0).
2. Open a Web browser on the client computer, and direct it to the default management module IP address (192.168.70.125).
3. Enter the default user name, USERID, and the default password, PASSW0RD (note the number zero, not the letter O, in PASSW0RD), to start the remote session.
4. Follow the instructions on the screen. Make sure that you set the timeout value that you want for your Web session.

After you connect the client computer to the Management Module 2 for the first time, perform the initial configuration of the Blade Server Chassis Enterprise SBCE.

Ethernet Connection (CLI)

After you connect the Ethernet cable from the Management Module 2 to the client computer, complete the following steps:

1. Make sure that the subnet of the client computer is set to the same value as the default management module subnet (255.255.255.0).
2. Open a console window and log in to the default management module IP address (192.168.70.125).
3. Enter the default user name, USERID, and the default password, PASSW0RD (note the number zero, not the letter O, in PASSW0RD), to start the remote session.

After you connect the client computer to the Management Module 2 for the first time, perform initial the configuration of the Blade Server Chassis Enterprise SBCE.

Serial Connection (CLI)

After you connect the serial cable from the Management Module 2 to the client computer, complete the following steps:

1. Make sure that the serial port of the client computer is set to the following settings:
   - Baud rate = 57600
   - Parity = none
   - Stop bits = 1
2. Open a terminal emulator window and establish a connection to the management module serial port.
3. Enter the default user name, USERID, and the default password, PASSW0RD (note the number zero, not the letter O, in PASSW0RD), to start the remote session.

After you connect to the Management Module 2 for the first time, perform initial configuration of the Blade Server Chassis Enterprise SBCE. See the *Intel*® Blade Server Chassis Enterprise SBCE*: Management Module Command-line Interface Reference Guide* for instructions.

4 Using the Management Module Web Interface

This section provides instructions for using the management module Web interface. It has the following information:

See Chapter 5, "Management Module Web Interface," on page 69 for a detailed description of the structure and content of the management module Web interface. Many Web interface functions can also be performed through the management module command-line interface (CLI). See the *Intel*® Blade Server Chassis Enterprise SBCE*: Management Module Command-line Interface Reference Guide* for information and instructions.

Connecting to the Management Module 2

A remote console connection to the Management Module 2 is required to configure and manage operation of the Blade Server Chassis Enterprise SBCE. All management module types support connection through the remote management and console (Ethernet) connector. The Chassis Management Module 2 also supports CLI-only connection through the serial management port.

You can manage the Intel® Blade Server Chassis Enterprise SBCE 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, a Secure Shell (SSH) server, or the serial port. All management connections to blade servers that do not support KVM are made through the management module command-line interface.

You can perform initial configuration of the Management Module 2 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 using a temporary connection. The following information is in this section:

After the initial cabling and configuration, connect to the Management Module 2 as described in "Starting the Management Module Web Interface" on page 27.

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

- A computer with Internet browser capability. To facilitate connections at multiple locations, you can use a notebook computer.
- The management module MAC address (listed on the label on the Management Module 2).
- For a networked connection to the Management Module 2, the following equipment:
  - A standard Ethernet cable
  - A local Ethernet network port (facility connection)
- For direct connection of a computer to the Management Module 2 remote management and console (Ethernet) connector, an Ethernet crossover cable. The Chassis Management Module 2 can use either a standard Ethernet cable or an Ethernet crossover cable to make this connection.

Connections through the advanced management module serial port can access only the management module command-line interface (CLI). For information about accessing the management module CLI, see the *Intel*® Blade Server Chassis Enterprise SBCE*: Management Module Command-line Interface Reference Guide*.

Hardware Requirements

To use the Remote Control feature that provides KVM access to a blade server, the client system must have, at minimum, the performance level of an Intel® Pentium® III or later microprocessor operating at 700 MHz or faster.

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

Resolution	Refresh Rate
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 2 supports the following Web browsers for remote (client) access. The client Web browser that you use must be Java* -enabled, must support JavaScript* version 1.2 or later, and must have the Java Virtual Machine (JVM) Plug-in between version 1.4.2_08 and version 1.5. The JVM Plug-in is available at http://www.java.com/.

- Microsoft Internet Explorer* 5.5 or later (with latest Service Pack installed)
- Netscape Navigator* 7.0 or later
- Mozilla* version 1.3 or later

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

- Microsoft Windows Server 2003*
- Microsoft Windows 2000* with Service Pack 4 or later
- Red Hat* Linux version 7.3
- SUSE* LINUX version 8.0
- Novell NetWare* 6.5

To use the Remote Control feature on an Chassis Management Module 2, the client system must also have the Sun JRE between version 1.4.2_08 and version 1.5.

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

Cabling the Management Module

The following sections describe how to cable the Management Module 2 to configure the Blade Server Chassis Enterprise SBCE by using the management module Web interface. See the *Installation Guide* for your Management Module 2 for specific cabling instructions. See the *Intel*® Blade Server Chassis Enterprise SBCE*: Management Module Command-line Interface Reference Guide* for information about connecting a remote console to the Management Module 2 and using the management module CLI to configure the Blade Server Chassis Enterprise SBCE.

After you cable the Management Module 2 for initial configuration, see "Connecting to the Management Module for the First Time" on page 26.

Networked Connection

Connect one end of a Category 5 or higher Ethernet cable to the remote management and console (Ethernet) connector on the Management Module 2. Connect the other end of the Ethernet cable to the facility network.

Direct Connection

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 on the Management Module 2. Connect the other end of the crossover cable to the Ethernet connector on the client computer.

Connecting to the Management Module for the First Time

The following sections describe how to connect a remote console to the Management Module 2 to perform initial configuration of the Blade Server Chassis Enterprise SBCE. The Management Module 2 has the following default network settings:

- IP address: 192.168.70.125
- 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 2 is configured to respond to DHCP first before using its static IP address.

The client computer that you connect to the Management Module 2 must be configured to operate on the same subnet as the Blade Server Chassis Enterprise SBCE Management Module 2. The IP address of the Management Module 2 must also be in the same local domain as the client computer. To connect to the Management Module 2 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 2 to the client computer, complete the following steps:

1. Make sure that the subnet of the client computer is set to the same value as the default Management Module 2 subnet (255.255.255.0).
2. Open a Web browser on the client computer, and direct it to the default management module IP address (192.168.70.125).
3. Enter the default user name, USERID, and the default password, 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 to the Management Module 2 for the first time, perform the initial configuration of the Blade Server Chassis Enterprise SBCE (see "Configuring the Management Module" on page 28).

Starting the Management Module Web Interface

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 defined for the Management Module 2 remote connection.

   The Enter Network Password page opens.
2. Type your user name and password. If you are logging in to the Management Module 2 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 2 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.

The Blade Server Chassis Enterprise SBCE management module Web-interface page opens. The content of this and all other Web-interface pages varies according to the type of Blade Server Chassis Enterprise SBCE that you are using and the firmware versions and options that are installed. See Chapter 5, "Management Module Web Interface," on page 69 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 illustration shows the Management Module 2 interface.

The upper-left corner 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 preceding examples, the login ID is USER1, and the primary management module is identified as SN#01 and is installed in management module bay 1.

Configuring the Management Module

You configure only the primary (active) management module. The redundant management module, if present, receives the configuration and status information automatically from the primary management module when necessary. The configuration information in this chapter applies to the primary management module, which might be the only management module in the Blade Server Chassis Enterprise SBCE.

If the Management Module 2 that you installed is a replacement for the only management module in the Blade Server Chassis Enterprise SBCE 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 63 for information about applying a saved configuration file.

The Blade Server Chassis Enterprise SBCE automatically detects the modules and blade servers that are installed and stores the vital product data (VPD). When the Blade Server Chassis Enterprise SBCE is started, the Management Module 2 automatically configures the remote management port of the Management Module 2 so that you can configure and manage Blade Server Chassis Enterprise SBCE components. You configure and manage Blade Server Chassis Enterprise SBCE components remotely by using the management module Web interface or the management module command-line interface (CLI).

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 2, using a Telnet interface or a Web browser. See the documentation that comes with each I/O module for information.*

For the active Management Module 2 to communicate with network resources and with the I/O modules in the Blade Server Chassis Enterprise SBCE, 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 2 (see "Networked Connection" on page 18 for information). The initial automatic management module configuration enables the network-management station to connect to the Management Module 2 to configure the port completely and to configure the rest of the Blade Server Chassis Enterprise SBCE.
- The internal Ethernet port (Ethernet 1) on the Management Module 2 for communication with the I/O modules (see "Networked Connection" on page 18 for information). Internal Ethernet ports for the Chassis Management Module 2 cannot be manually configured.
- The management port on each I/O module that provides for communication with the Management Module 2. You configure this port by configuring the IP address for the I/O module (see "Connecting the Management Module 2 to the Network" on page 17 for information).

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

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

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

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

Configuring the Management Module for Remote Access

After you connect the active Management Module 2 to the network, the Ethernet port connection is configured in one of the following ways:

- If you have an accessible, active, and configured dynamic host configuration protocol (DHCP) server on the network, IP address, gateway address, subnet mask, and DNS server IP address are set automatically. The host name is set to the management module MAC address by default, and the domain server cannot change it.
- If the DHCP server does not respond within 3 minutes after the port is connected, the Management Module 2 uses the factory-defined static IP address and default subnet address.

Important: *You cannot connect to the Management Module 2 using the factory-defined static IP address and default subnet address until after this 3-minute period passes.*

Either of these actions enables the Ethernet connection on the active Management Module 2.

Make sure that the client computer is on the same subnet as the Management Module 2; then, use your Web browser to connect to the Management Module 2 (see "Starting the Management Module Web Interface" on page 27 for more information). In the browser **Address** field, specify the IP address that the Management Module 2 is using:

- If the IP address was assigned through a DHCP server, get the IP address from your network administrator.
- The factory-defined static IP address is 192.168.70.125, the default subnet address is 255.255.255.0, and the default host name is MM*xxxxxxxxxxxx*, where *xxxxxxxxxxxx* is the burned-in medium access control (MAC) address. The MAC address is on a label on the Management Module 2, below the IP reset button.

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

Configuring the Management Module Ethernet Ports

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

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

Note: *For I/O-module communication with a remote management station, the I/O-module internal network interface and the management module internal and external interfaces must be on the same subnet.*

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

✧ **Interface** - Select **Enabled** (the default) to use the Ethernet connection. (For the Chassis Management Module 2, this field is for information only and cannot be changed.)

✧ **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).

✧ **Hostname** - (Optional) This is the IP host name that you want to use for the Management Module 2 (maximum of 63 characters and following host-naming standards).

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

- IP address - The IP address for the Management Module 2. The IP address must contain four integers from 0 through 255, separated by periods, with no spaces or consecutive periods. The default setting is 192.168.70.125.
- Subnet mask - Four integers from 0 through 255, separated by periods, with no spaces. The default setting is 255.255.255.0.
- Gateway address - The IP address for your network gateway router. The gateway address must contain four integers from 0 through 255, separated by periods, with no spaces. This address must be accessible from the IP address and subnet mask.

— **Advanced Ethernet Setup** - View the data rate, duplex mode, maximum transmission (MTU), locally-administered MAC address, and burned-in MAC address for this interface. You can configure the locally administered MAC address; the other fields are read-only.

3. Configure the internal Ethernet management port on each I/O module in the Blade Server Chassis Enterprise SBCE.

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

a. Under **I/O Module Tasks** in the navigation pane, click **Configuration**.

a. Click **Bay 1**.

b. In the **New Static IP address** fields, specify the IP configuration to use for this interface. The subnet mask must be the same as the subnet mask in the internal network interface (eth1).

c. Click **Advanced Configuration**.

d. In the **Advanced Setup** section, enable external management over all ports.

e. Under **I/O Module Tasks** in the navigation pane, click **Admin/Power/Restart**.

f. 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)*

Repeat step 3 for each I/O module in the Blade Server Chassis Enterprise SBCE.

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.

See the *Intel® Blade Server Chassis Enterprise SBCE: Management Module User's Guide* for more information about the management module Web interface.

Configuring Advanced Features

The following sections provide instructions for performing some of the functions that the management module Web interface supports. Detailed descriptions of the management module Web interface are in Chapter 5, "Management Module Web Interface," on page 69.

- "Network and Security Configuration" on page 32
- "Configuring Wake on LAN" on page 60
- "Using the Configuration File" on page 62
- "Using the Remote Disk Feature" on page 66

Network and Security Configuration

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

- SNMP and DNS (see "Configuring SNMP" on page 32)
- SMTP (see "Configuring SMTP" on page 36)
- SSL and LDAP (see "Configuring LDAP" on page 36)
- SSH (see "Configuring the Secure Shell Server" on page 58)

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 2, you must install and compile the management information base (MIB) on your SNMP manager. The MIB supports SNMP traps. The MIB is included in the management module firmware update package that you downloaded from the Intel Support Web site.*

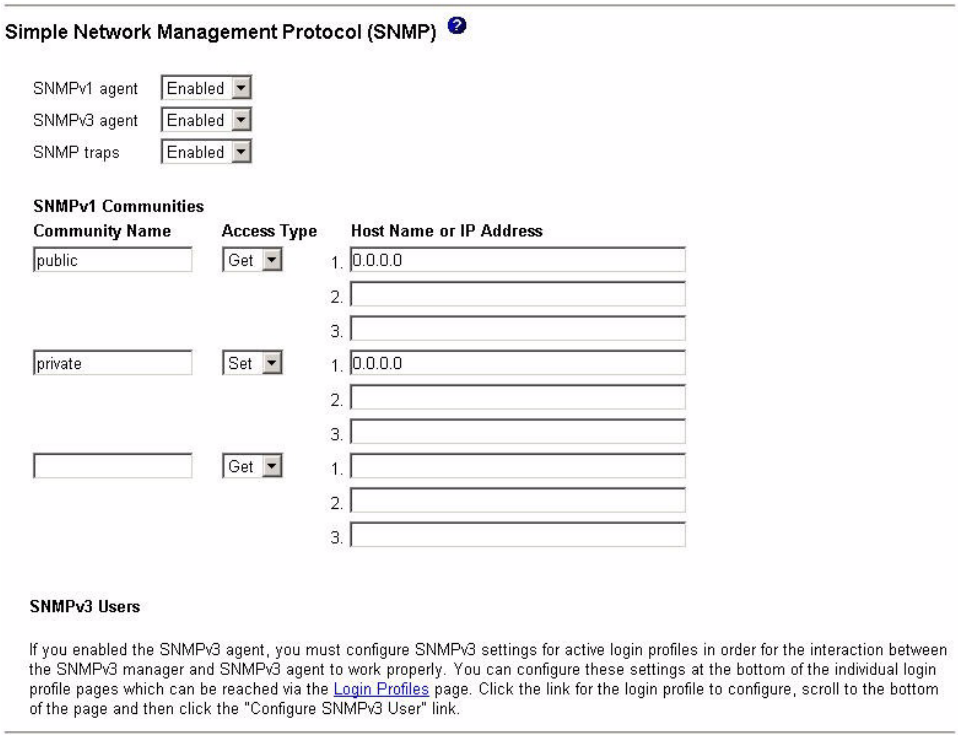
To configure SNMP, complete the following steps:

1. Log in to the Management Module 2 on which you want to configure SNMP. For more information, see "Starting the Management Module Web Interface" on page 27.
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 2. The name will be included with e-mail and SNMP alert notifications to identify the source of the alert. If more than one Management Module 2 is installed in a Blade Server Chassis Enterprise SBCE, each Management Module 2 can be given a unique name.

— **Contact** - The name and phone number of the person to contact if there is a problem with the Blade Server Chassis Enterprise SBCE.

— **Location** - Sufficient detail to quickly locate the Blade Server Chassis Enterprise SBCE 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. 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.

Note: *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 this SNMP agent.*

   a. In the **Community Name** field, enter a name or authentication string to specify the community.

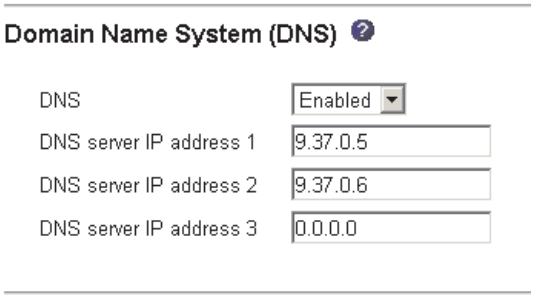
   b. Select the **Access Type** for the community.

   c. In the corresponding **Host Name** or **IP Address** field, enter the host name or IP address of each community manager.

7. Complete one of the following, based on DNS server availability:

   — If a DNS server is not available on your network, scroll to the bottom of the page and click **Save**.

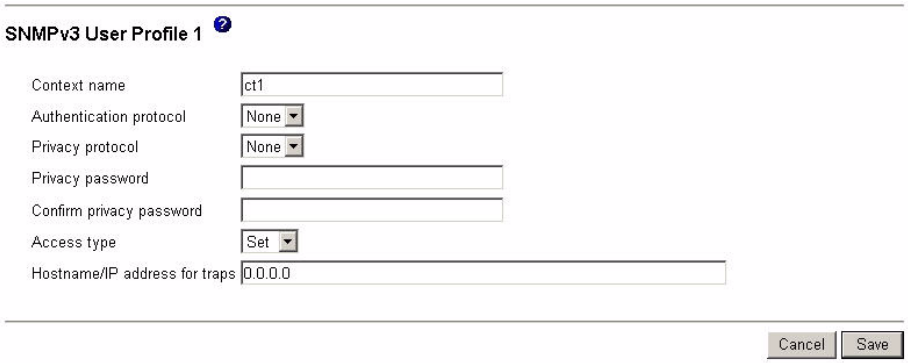
   — If a DNS server is available on your network, scroll to the **Domain Name System (DNS)** section. A page similar to the one in the following illustration is displayed.



8. If a DNS server (or servers) is available on your network, select **Enabled** in the **DNS** field.

   The **DNS** field specifies whether you use a DNS server on your network to translate host names into IP addresses.

9. (Optional) If you enabled DNS, in the **DNS server IP address** fields, specify the IP addresses of up to three DNS servers on your network. Each IP address must contain four integers from 0 through 255, separated by periods.
10. Scroll to the bottom of the page and click **Save**.
11. If you are enabling the SNMPv3 agent, complete the following steps to configure the SNMPv3 profile for each SNMPv3 user; otherwise, continue with step 12.
    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.



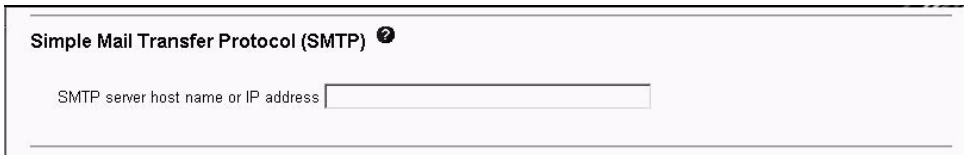
    c. Specify the SNMPv3 configuration information for this user; then, click **Save**.
    d. Repeat step b and step c for each SNMPv3 user.
12. In the navigation pane, click **MM Control → Restart MM**; then, restart the Management Module 2 to activate the changes.

Configuring SMTP

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 e-mail 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 as part of an e-mail address (for example, there are no spaces).*

1. Log in to the Management Module 2 on which you want to configure SMTP. For more information, see "Starting the Management Module Web Interface" on page 27.
2. In the navigation pane, click **MM Control → Network Protocols**, and scroll down to the **Simple Mail Transfer Protocol (SMTP)** section.



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

Configuring LDAP

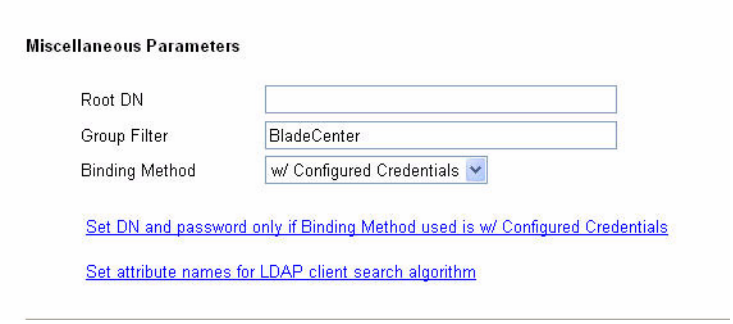
Using a Lightweight Directory Access Protocol (LDAP) server, a Management Module 2 can authenticate a user by querying or searching an LDAP directory on an LDAP server, instead of going through its local user database. Then, all LDAP clients (Blade Server Chassis Enterprise SBCE management modules or server Remote Supervisor Adapters) can remotely authenticate any user access through a central LDAP server. This requires LDAP client support on the Management Module 2. You can also assign authority levels according to information that is found on the LDAP server.

You can also use LDAP to assign users and management modules to groups and perform group authentication, in addition to the normal user (password check) authentication. For example, a Management Module 2 can be associated with one or more groups, and a user would pass only group authentication if the user belongs to at least one group that is associated with the Management Module 2.

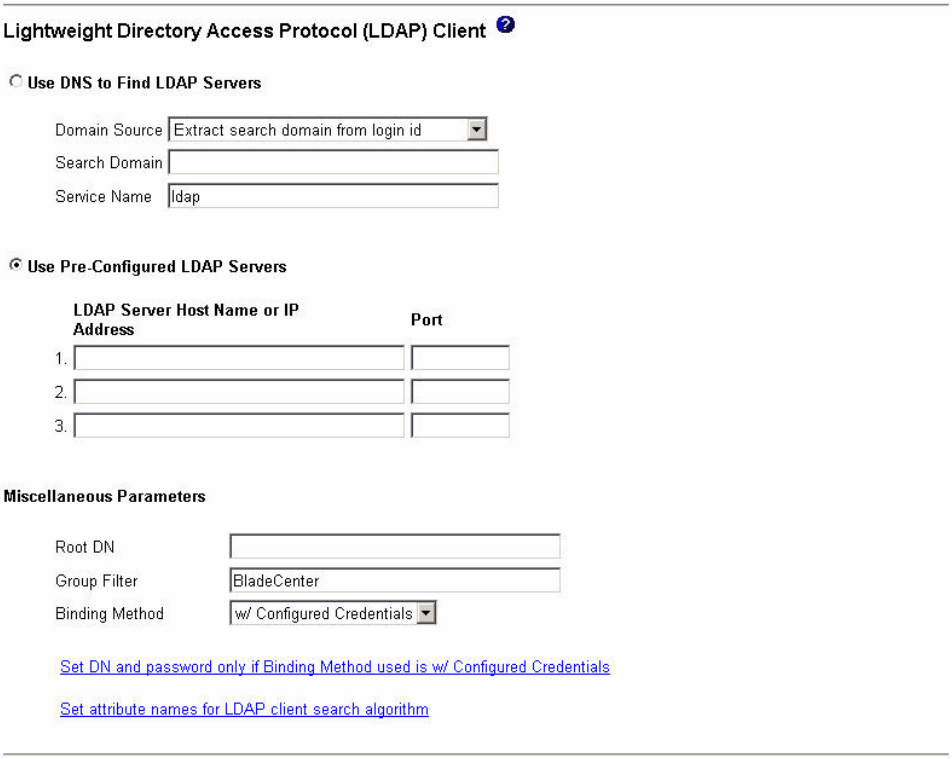
Setting up a Client to Use the LDAP Server

To set up a client to use the LDAP server, complete the following steps:

1. Log in to the Management Module 2 on which you want to set up the client. For more information, see "Starting the Management Module Web Interface" on page 27.
2. In the navigation pane, click **MM Control → Network Protocols**. Scroll down to the **Lightweight Directory Access Protocol (LDAP) Client** section. For management modules other than the Chassis Management Module 2, a page similar to the one in the following illustration is displayed.



For the Chassis Management Module 2, a page similar to the one in the following illustration is displayed.



For the Chassis Management Module 2, a page similar to the one in the following illustration is displayed.

3. Configure the LDAP client, using the following information:

   a. For an Chassis Management Module 2, select **Use DNS to find LDAP Servers** or **Use Pre-Configured LDAP Servers** (default).

      The Management Module 2 contains a Version 2.0 LDAP Client that you can configure to provide user authentication through one or more LDAP servers. For the Chassis Management Module 2, the LDAP servers that are used for authentication can be discovered dynamically or manually preconfigured. For management modules other than the Chassis Management Module 2, the LDAP servers that are used for authentication are manually preconfigured.

   b. If you are using DNS to find LDAP servers, configure the following settings; then, go to step d. When discovering LDAP servers dynamically, the mechanisms that are described by RFC2782 are applied to find the servers through a process called DNS SRV.

      - Domain Source

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

        - **Extract search domain from login id**. The LDAP client uses the domain name in the login ID. For example, if the login ID is joesmith@mycompany.com, the domain name is mycompany.com. If the domain name cannot be extracted from the login ID, the DNS SRV process fails, causing a user authentication failure.
        - **Use only configured search domain below**. The LDAP client uses the domain name that is set in the **Search Domain** field.
        - **Try login id first, then configured value**. The LDAP client first attempts to extract the domain name from the login ID. If this succeeds, this domain name is used in the DNS SRV request. If there is no domain name in the login ID, the LDAP client uses the domain name that is set in the **Search Domain** field as the domain name in the DNS SRV request. If neither of these items is configured, user authentication fails.

      - Search Domain

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

      - Service Name

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

   c. If you are using preconfigured LDAP servers, configure the **LDAP Server** fields (for management modules other than the Chassis Management Module 2) or the **LDAP Server Host Name or IP Address** fields (for the Chassis Management Module 2); then, go to step d.

The port number for each server is optional. If the field is left blank, the default value of 389 is used for nonsecured LDAP connections. For secured connections, the default is 636. You must configure at least one LDAP server.

d. Configure the following items for all LDAP server types:

- ✧ Root DN

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

- ✧ User Search Base DN

  (For management modules other than the Chassis Management Module 2) As part of the user authentication process, the LDAP server must be searched for one or more attributes that are associated with a particular user. Any search request must specify the base distinguished name for the actual search. The **User Search Base DN** field specifies the base distinguished name that is used to search the user directory (for example, cn=Users,dn=companyABC,dn=com). If this field is left blank, the root distinguished name is used as the search base.

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

- ✧ Group Filter

  This parameter is used for group authentication. It specifies the set of groups to which the Management Module 2 belongs. If this field is left blank, group authentication is disabled. Otherwise, group authentication is performed against this filter. The specified filter can be a specific group name (for example, MarketingWest), a wildcard with a prefix (for example, Marketing*), or a wildcard (specified as *). If a specific name is used, the Management Module 2 belongs only to that group. If a prefix filter is used (for example, Mar*), the Management Module 2 belongs to any group whose first three letters are Int. If a wildcard filter (*) is used, the Management Module 2 belongs to all groups. The default filter is Mar*.

  – Group authentication is performed after user authentication (where a user ID and password are verified). Group authentication refers to the process of verifying that a user is a member of at least one group that is associated with the Management Module 2. For example, if the group filter is set to Mar* and the user belongs to two groups (for example, Engineering and MarkegingWest), group authentication passes because the user belongs to a group (MarketingWest) that matches the filter Mar*. If the groups to which the user belongs do not match the filter, group authentication fails, and the user is not allowed to access the Management Module 2. Note that if the group filter is *, group authentication will automatically succeed because any group to which the user belongs will match this wildcard.

- ✧ Binding Method

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

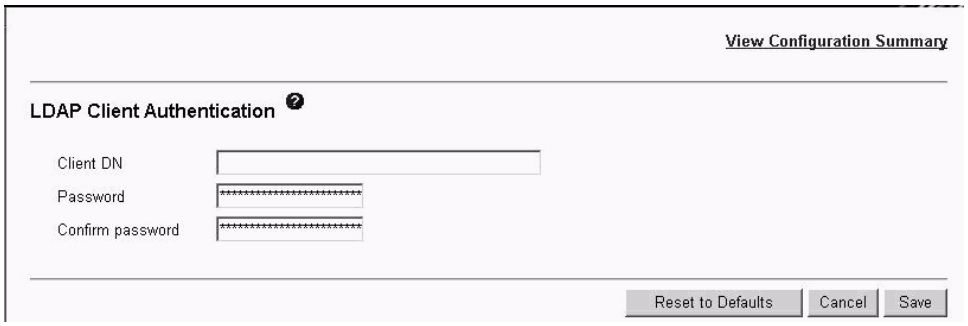
  - **Anonymous authentication**. A bind attempt is made without a client distinguished name or password. If the bind is successful, a search will be requested to find an entry on the LDAP server for the user who is attempting to log in. If an entry is found, a second attempt to bind is attempted, this time with the distinguished name and password of the user. If this succeeds, the user has passed the user authentication phase. Group authentication is then attempted, if it is enabled.
  - **w/ Configured Credentials**. A bind attempt is made, using the configured client domain name and password. If the initial bind is successful, a search is performed to find an entry on the LDAP server that belongs to the user who is logging in. If necessary, a second attempt to bind is attempted, this time with the domain name that is retrieved from the user LDAP record and the password that was entered during the login process. If this fails, the user is denied access.
  - **w/ Login Credentials**. A bind attempt is made, using the credentials that were supplied during the login process. If the initial bind is successful, a search is performed to find an entry on the LDAP server that belongs to the user who is logging in.

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

Configuring the LDAP Client Authentication

To configure the LDAP client authentication, 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 and click **Set DN and password for Client Authentication**. A page similar to the one in the following illustration is displayed.

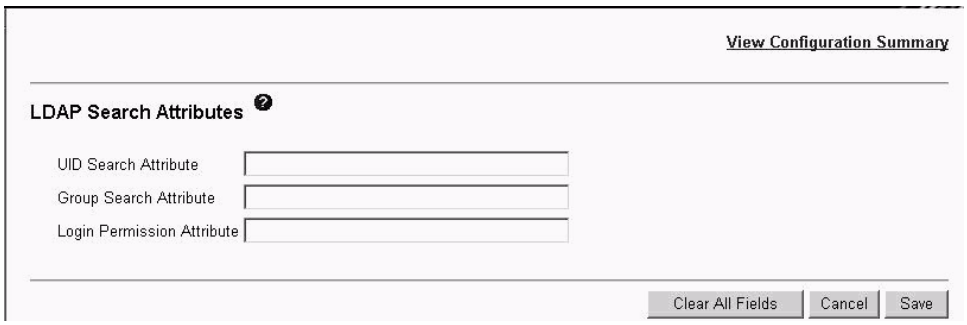


3. Perform the initial bind to the LDAP server during user authentication with anonymous authentication, client-based authentication, or user principal name. To use client-based authentication, in the **Client DN** field, type a client distinguished name. Type a password in the **Password** field or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

Configuring the LDAP Search Attributes

To configure the LDAP search attributes, 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 and click **Set search attribute names for LDAP based authentication**. A page similar to the one in the following illustration is displayed.



3. To configure the search attributes, use the following information:
   - ✧ UID Search Attribute

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

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

   - ✧ Group Search Attribute

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

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

   - ✧ Login Permission Attribute

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

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

– The field supports user roles for both the command authorities that are used in earlier versions of management module firmware and the role-based user permissions for the latest version of management module firmware. Bit positions 11 through 16 determine which type of role is used. See "Web Interface Pages and User Roles" on page 70 for information about the commands available for each user role.

– The attribute value must be a bit string that is entered as consecutive zeros or ones, with each bit representing a particular set of functions (for example, 010000000000 or 0000110010000). The bits are numbered according to their positions. The leftmost bit is bit position 0, and the rightmost bit is bit position 50. A value of 1 at a particular position enables the corresponding function. A value of 0 disables that function. The LDAP attribute string is copied into a local string that is 64 characters long. If fewer than 64 characters are specified, the local string is padded with zeros. If the string is longer than 64 characters, extra characters are not copied.

The following functions are associated with the 50-bit positions:

Table 2. Bit Positions and Functions

Bit Position	Description	Function
0 through 10	User authorities	Ror scripting on management modules other than the Chassis Management Module 2
0	Deny Always	If this bit is set, a user will always fail authentication. This function can be used to block a particular user or users who are associated with a particular group
1	Supervisor Access	If this bit is set, a user is given administrator privileges. The user has read and write access to every function. When this bit is set, other bits that define specific function access do not have to be set individually.
2	Read Only Access	If this bit is set, a user has read-only access and cannot perform any maintenance procedures (for example, restart, remote actions, and firmware updates), and nothing can be modified (using the save, clear, or restore functions). Note that read-only and all other bits are mutually exclusive, with bit position 2 having the lowest precedence. That is, if any other bit is set, this bit is ignored
3	Networking and Security	If this bit is set, a user can modify the settings in the Security, Network Protocols, and Network Interface pages for MM Control. If this bit is set, a user can also modify the settings in the Management page for I/O Module Tasks

Table 2. Bit Positions and Functions (Cont'd)

Bit Position	Description	Function
4	User Account Management	If this bit is set, a user can add, modify, and delete users and change the Global Login Settings in the Login Profiles page
5	Blade server Remote Console Access	If this bit is set, a user can access the remote server console
6	Blade server Remote Console and Virtual Media Access	If this bit is set, a user can access the remote server console and the virtual media functions for the remote server.
7	Blade and I/O Module Power/ Restart Access	If this bit is set, a user can access the power-on and restart functions for the blade servers and I/O modules.
8	Basic Configuration (MM, I/O Modules, Blades)	If this bit is set, a user can modify the General Settings and Alerts pages for MM Control and the Configuration page for Blade Tasks
9	Ability to Clear Event Logs	If this bit is set, a user can clear the event logs. Everyone can look at the event logs, but this permission is required to clear the logs.
10	Advanced Configuration (MM, I/O Modules, Blades)	If this bit is set, a user has no restrictions when configuring the Management Module 2, blade servers, I/O modules, and VPD. The user can also perform firmware upgrades on the Management Module 2 or blade servers, restore the Management Module 2 to its factory default settings, modify and restore the management module configuration from a configuration file, and restart or reset the Management Module 2
11 through 15	Permission version	These bits specify which type of user roles, user authorities, or role-based user permissions is being used. If these bits are set to 00001, the role-based user permissions, using bits 16 through 30, are used. If these bits are set to 00000 or any other value, the user authorities, using bits 0 through 10, are used.
16 through 30	Role-based user permissions	Non-scripting use on all management module types
16	Deny Always	If this bit is set, a user will always fail authentication. This function can be used to block a particular user or users who are associated with a particular group.
17	Supervisor	If this bit is set, a user is given administrator privileges. The user has read and write access to every function. When this bit is set, other bits that define specific function access do not have to be set individually.

Table 2. Bit Positions and Functions (Cont'd)

Bit Position	Description	Function
18	Operator	If this bit is set, a user can view all information. User access to information is limited by the permission scope that is specified in bits 31 through 49
19	Chassis Operator	If this bit is set, a user can view information about the common Blade Server Chassis Enterprise SBCE components.
20	Chassis User Account Management	If this bit is set, a user can add, modify, and delete user login profiles. Changing the Global Login Settings requires Chassis Configuration permission.
21	Chassis Log Management	If this bit is set, a user can clear the event logs or change the log policy settings. All users can look at the event logs, but this permission is required to clear the logs or change the log policy settings at the top of the event-log page
22	Chassis Configuration	If this bit is set, a user can perform management and setup operations for the common Blade Server Chassis Enterprise SBCE components and features. User access to information is limited by the permission scope that is specified in bit 45.
23	Chassis Administration	If this bit is set, a user can manage operation of the common Blade Server Chassis Enterprise SBCE components and features. User access to information is limited by the permission scope that is specified in bit 45.
24	Blade Operator	If this bit is set, a user can view information about the blade servers. User access to blade servers is limited by the permission scope that is specified in bits 31 through 44.
25	Blade Remote Presence	If this bit is set, a user can access the remote server console and the virtual media functions for the remote server. User access to blade servers is limited by the permission scope that is specified in bits 31 through 44.
26	Blade Configuration	If this bit is set, a user can perform management and setup operations for the blade servers. User access to blade servers is limited by the permission scope that is specified in bits 31 through 44.
27	Blade Administration	If this bit is set, a user can manage operation of the blade servers. User access to blade servers is limited by the permission scope that is specified in bits 31 through 44.
28	Switch Operator	If this bit is set, a user can view information about the I/O modules. User access to I/O modules is limited by the permission scope that is specified in bits 46 through 55.

Table 2. Bit Positions and Functions (Cont'd)

Bit Position	Description	Function
29	Switch Module Configuration	If this bit is set, a user can perform management and setup operations for the I/O modules. User access to I/O modules is limited by the permission scope that is specified in bits 46 through 55.
30	Switch Module Administration	If this bit is set, a user can manage operation of the I/O modules. User access to I/O modules is limited by the permission scope that is specified in bits 46 through 55
31 through 55	Permission scope	For role-based user permissions
31	Blade 1	If this bit is set, a user can access information about the blade server that is addressed in blade bay 1
32	Blade 2	Blade 2 (bit position 32): If this bit is set, a user can access information about the blade server that is addressed in blade bay 2
33	Blade 3	If this bit is set, a user can access information about the blade server that is addressed in blade bay 3.
34	Blade 4	If this bit is set, a user can access information about the blade server that is addressed in blade bay 4.
35	Blade 5	If this bit is set, a user can access information about the blade server that is addressed in blade bay 5.
36	Blade 6	If this bit is set, a user can access information about the blade server that is addressed in blade bay 6
37	Blade 7	If this bit is set, a user can access information about the blade server that is addressed in blade bay 7.
38	Blade 8	If this bit is set, a user can access information about the blade server that is addressed in blade bay 8.
39	Blade 9	If this bit is set, a user can access information about the blade server that is addressed in blade bay 9.
40	Blade 10	If this bit is set, a user can access information about the blade server that is addressed in blade bay 10.
41	Blade 11	If this bit is set, a user can access information about the blade server that is addressed in blade bay 11.
42	Blade 12	If this bit is set, a user can access information about the blade server that is addressed in blade bay 12.

Table 2. Bit Positions and Functions (Cont'd)

Bit Position	Description	Function
43	Blade 13	If this bit is set, a user can access information about the blade server that is addressed in blade bay 13
44	Blade 14	If this bit is set, a user can access information about the blade server that is addressed in blade bay 14.
45	Chassis	If this bit is set, a user can access information about the common Blade Server Chassis Enterprise SBCE components.
46	I/O Module 1	If this bit is set, a user can access information about the I/O module in I/O module bay 1.
47	I/O Module 2	If this bit is set, a user can access information about the I/O module in I/O module bay 2.
48	I/O Module 3	If this bit is set, a user can access information about the I/O module in I/O module bay 3.
49	I/O Module 4	If this bit is set, a user can access information about the I/O module in I/O module bay 4.
50	I/O Module 5	If this bit is set, a user can access information about the I/O module in I/O module bay 5.
51	I/O Module 6	If this bit is set, a user can access information about the I/O module in I/O module bay 6.
52	I/O Module 7	If this bit is set, a user can access information about the I/O module in I/O module bay 7.
53	I/O Module 8	If this bit is set, a user can access information about the I/O module in I/O module bay 8.
54	I/O Module 9	If this bit is set, a user can access information about the I/O module in I/O module bay 9.
55	I/O Module 10	If this bit is set, a user can access information about the I/O module in I/O module bay 10.
56 through 63	Reserved	These bits are reserved for future use

If none of the bits are set, the default is read-only for the user.

Priority is given to login permissions that are retrieved directly from the user record. If the user record does not have the login permission attribute, an attempt will be made to retrieve the permissions from the groups to which the user belongs. This is done as part of the group authentication phase. The user will be assigned the inclusive OR of all the bits for all of the groups. The Browser Only bit is set only if all the other bits are set to zero. If the Deny Always bit is set for any of the groups, the user will be refused access. The Deny Always bit always has precedence over every other bit.

Secure Web Server and Secure LDAP

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

You can configure the Management Module 2 to use SSL support for two types of connections: secure Web server (HTTPS) and secure LDAP connection (LDAPS). The Management Module 2 takes on the role of SSL client or SSL server, depending on the type of connection. The following table shows that the Management Module 2 acts as an SSL server for secure Web server connections. The Management Module 2 acts as an SSL client for secure LDAP connections.

Table 3. Management Module SSL Connection Support

Connection Type	SSL Client	SSL Server
Secure Web server (HTTPS)	Web browser of the user (for example, Microsoft Internet Explorer)	Management Module Web server
Secure LDAP connection (LDAPS)	Management Module LDAP client	An LDAP server

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

Configuring Security

Use the general procedure in this section to configure security for the management module Web server and to configure security for the connection between the Management Module 2 and an LDAP server. If you are not familiar with the use of SSL certificates, read the information in "SSL Certificate Overview" on page 48.

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 2:

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 49.)
   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 55.)

2. Configure the SSL client certificates for secure LDAP connections:
   a. Disable the SSL client. Use the **SSL Client Configuration for LDAP Client** section on the **MM Control → Security** page.
   b. Generate or import a certificate. Use the **SSL Client Certificate Management** section on the **MM Control → Security** page. (See "SSL Client Certificate Management" on page 55.)
   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 55.)
   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 57.)
3. Restart the Management Module 2 for SSL server configuration changes to take effect. For more information, see "Power/Restart" on page 85.

Note: *Changes to the SSL client configuration take effect immediately and do not require a restart of the Management Module 2.*

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 risk arises because 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. It is possible that a third party could impersonate the server and intercept data that moves between the Management Module 2 and the Web browser. If, at the time of the initial connection between the browser and the Management Module 2, the self-signed certificate is imported into the certificate store of the browser, all future communications will be 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 2 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 2. A certificate contains digital signatures for the certificate authority and the Management Module 2. 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 is able to validate the certificate and positively identify the management module Web server.

The Management Module 2 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.

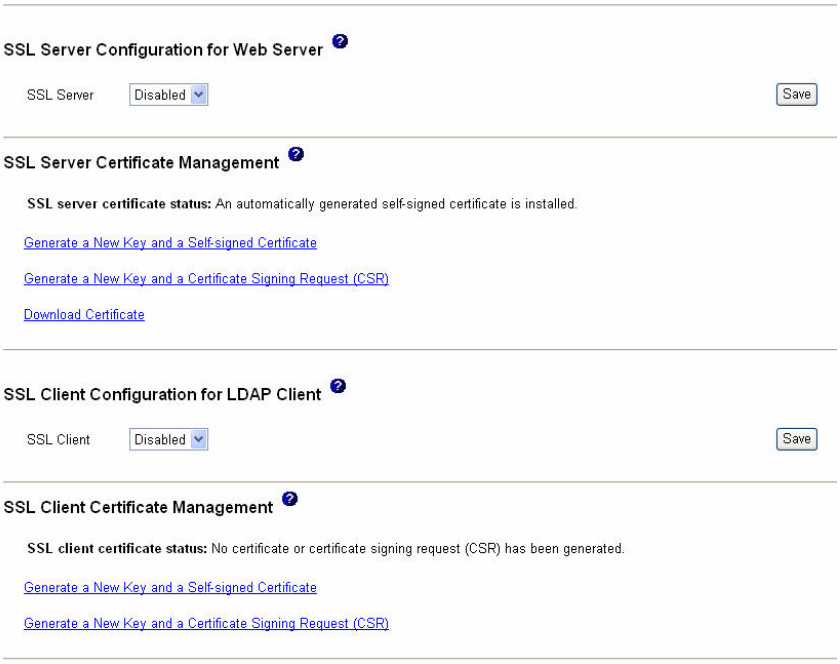
SSL Server Certificate Management

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. If you want to use a self-signed certificate for the SSL server, see "Generating a Self-signed Certificate" on page 49. If you want to use a certificate-authority-signed certificate for the SSL server, see "Generating a Certificate Signing Request" on page 51.

Generating a Self-signed Certificate

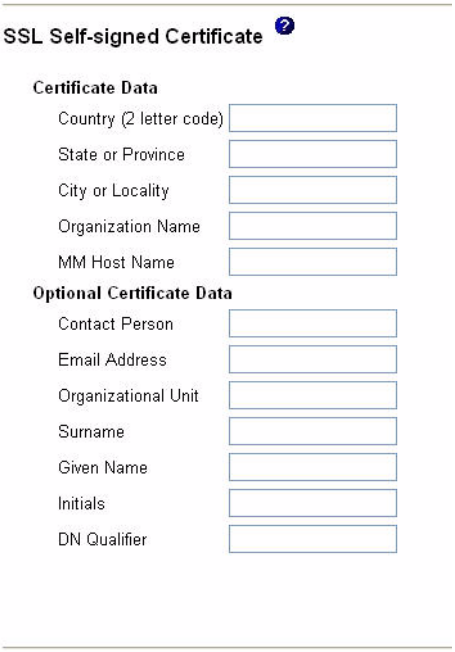
To generate a new private encryption key and self-signed certificate, complete the following steps:

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



2. In the **SSL Server Configuration for Web Server** section, make sure that the SSL server is disabled. If it is not disabled, select **Disabled** in the **SSL Server** field and then click **Save**.

3. In the **SSL Server Certificate Management** section, select **Generate a New Key and a Self-signed Certificate**. A page similar to the one in the following illustration is displayed.



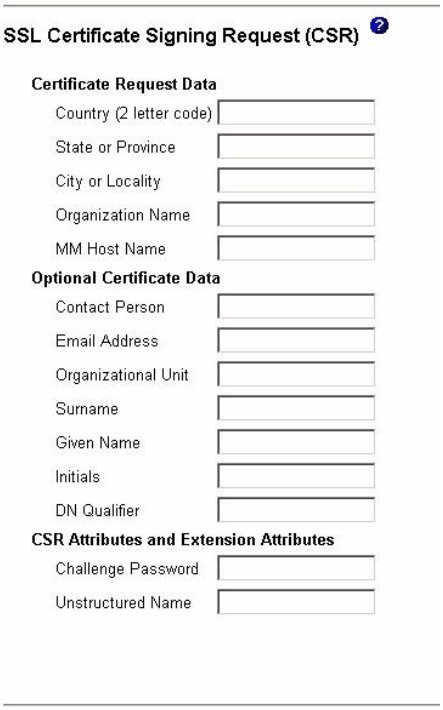
4. Type the information in the required fields and any optional fields that apply to your configuration. For a description of the fields, see “Required certificate data” on page <xref>451 After you finish typing the information, click **Generate Certificate**. Your new encryption keys and certificate 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 and then click **Save**.
3. In the **SSL Server Certificate Management** section, select **Generate a New Key and a Certificate Signing Request**. A page similar to the one in the following illustration is displayed.



4. Type the information in the required fields and any optional fields that apply to your configuration. The fields are the same as 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 2 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 2 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 2 is located. This field can contain a maximum of 50 characters.
- Organization Name: Use this field to indicate the company or organization that owns the Management Module 2. 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 that appears 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 2. 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.

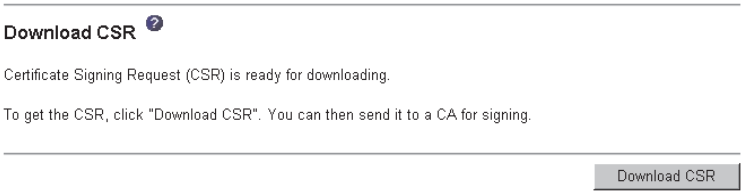
✧ Optional certificate dataless following user-input fields are optional for generating a self-signed certificate or a certificate-signing request:
- Contact Person: Use this field to indicate the name of a contact person who is responsible for the Management Module 2. This field can contain a maximum of 60 characters.
- Email Address: Use this field to indicate the e-mail address of a contact person who is responsible for the Management Module 2. This field can contain a maximum of 60 characters.
- Organizational Unit: Use this field to indicate the unit within the company or organization that owns the Management Module 2. 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 2. 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 2. 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 2. 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 2. This field can contain a maximum of 60 characters.
- Years Valid: This field is present for only 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 2. This field can contain a maximum of 60 characters.

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



6. Click **Download CSR** and then click **Save** to save the file to your 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
   ```

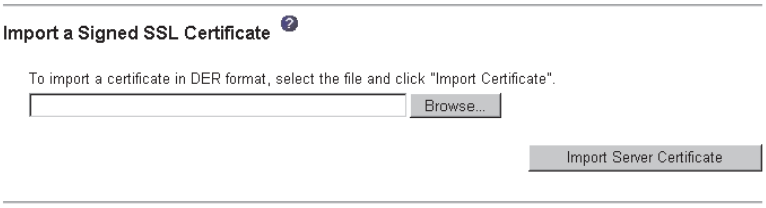
7. Send the certificate signing request to your certificate authority. When the certificate authority returns your signed certificate, you might have to convert the certificate to DER format. (If you received the certificate as text in an e-mail or a Web page, it is probably in PEM format.) You can change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

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

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

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

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



10. Click **Browse**.
11. Click the certificate file that you want and then click **Open**. The file name (including the full path) is displayed in the field next to the **Browse** button.
12. Click **Import Server Certificate** to begin the process. A progress indicator is displayed as the file is transferred to storage on the Management Module 2. Continue displaying this page until the transfer is completed.

Enabling SSL for the Secure Web Server

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

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, go to "SSL Server Certificate Management" on page 49.

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

SSL Client Certificate Management

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

The procedure for generating the private encryption key and certificate for the SSL client is the same as the procedure for the SSL server, except that you use the **SSL Client Certificate Management** section of the Security Web page instead of the **SSL Server Certificate Management** section. If you want to use a self-signed certificate for the SSL client, see "Generating a Self-signed Certificate" on page 49. If you want to use a certificate-authority-signed certificate for the SSL client, see "Generating a Certificate Signing Request" on page 51.

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 2 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 and then click **Save**.

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

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

5. Click **Browse**.
6. Select the certificate file that you want and click **Open**. The file name (including the full path) is displayed in the box next to the **Browse** button.
7. To begin the import process, click **Import Certificate**. A progress indicator is displayed as the file is transferred to storage on the Management Module 2. Continue displaying this page until the transfer is completed.

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

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

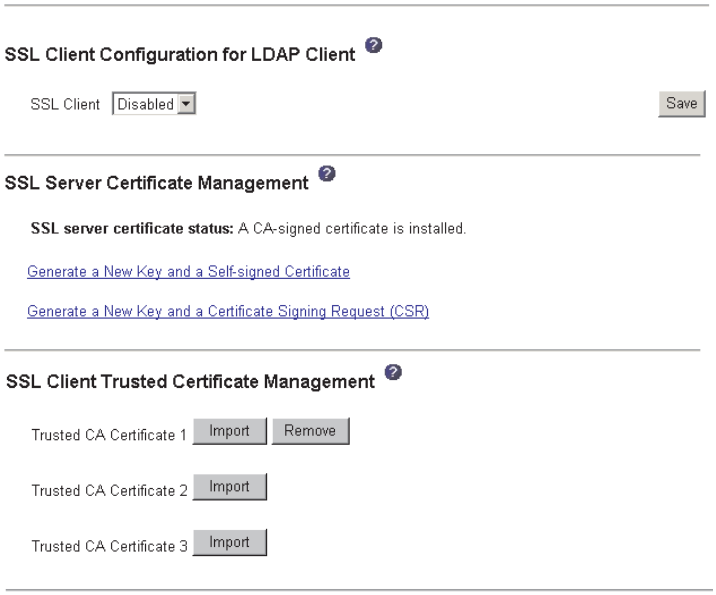
You can import other trusted certificates by using the Trusted CA Certificate 2 and the Trusted CA Certificate 3 **Import** buttons.

Enabling SSL for the LDAP Client

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

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

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



   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 Server

The Secure Shell (SSH) feature provides secure access to the command-line interface and the Serial over LAN (text console) redirect features of the Management Module 2.

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

Generating a Secure Shell Server Key

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

When you request a new server key, both an RSA key and a DSA key are created to allow access to the Management Module 2 from either an SSH version 1.5 or an SSH version 2 client. For security, the Secure Shell server private key is not backed up during a configuration save and restore operation.

The following 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 Red Hat* Linux 7.3 was used to test the command-line interface.
- The SSH client of cygwin (see http://www.cygwin.com for information).

The following table shows the types of encryption algorithms that are supported by the SSH version 1.5 and version 2.0.

.

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

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

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

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

Enabling the Secure Shell Server

From the Security page, you can enable or disable the Secure Shell server. The selection that you make takes effect only after the Management Module 2 is restarted. The value that is displayed on the screen (Enabled or Disabled) is the last selected value and is the value that is used when the Management Module 2 is restarted.

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

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

1. In the navigation pane, click **Security**.
2. Scroll to the **Secure Shell (SSH) Server** section. A page similar to the one in the following illustration is displayed.

3. Click **Enabled** in the **SSH Server** field.
4. In the navigation pane, click **Restart ASM** to restart the Management Module 2.

Using the Secure Shell Server

If you are using the Secure Shell client that is included in Red Hat Linux version 7.3, to start a Secure Shell session to a Management Module 2 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 user ID USERID.

Configuring Wake on LAN

To configure the Wake on LAN* feature in the Blade Server Chassis Enterprise SBCE, 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 VPD that the Management Module 2 maintains for each installed blade server. (Go to **Monitors → Hardware VPD** in the management module Web interface, and then scroll to the Blade Server Chassis Enterprise SBCE **Server MAC Addresses** section.)
   - 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 that has the MAC addresses printed on it.
   - 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 Blade Server Chassis Enterprise SBCE Management Module 2 (**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 Blade Server Chassis Enterprise SBCE 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 diskette into a USB attached diskette drive, and then restart the blade server.
5. When the A:\ prompt appears, 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 or Blade Server Chassis Enterprise SBCE 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

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

Note: *If you cannot communicate with a replacement Management Module 2 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 2 to the factory default IP addresses; then, access the Management Module 2 by using the factory IP address and configure the Management Module 2 or load the saved configuration file.*

Backing up your Management Module Configuration

The Management Module 2 allows you to save your management module configuration to a file. The Chassis Management Module 2 also allows you to save the management module configuration to the backplane of the Blade Server Chassis Enterprise SBCE.

The Management Module 2 and Chassis Management Module 2 have different backup procedures. They are described in the following sections.

You can download a copy of your current management module configuration to the client computer that is running the management module Web interface. Use this backup copy to restore your management module configuration if it is accidentally changed or damaged. Use it as a base that you can modify to configure multiple management modules with similar configurations.

Backing up a Management Module Configuration

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 27.
2. In the navigation pane, click **MM Control → Configuration File**.
3. In the **Backup MM Configuration** section, click **view the current configuration summary**.

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

Backing up an Chassis Management Module 2 Configuration

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 27.
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
4. If you are saving the configuration to the chassis, click **Save**.
5. If you are restoring the configuration from a file, click **view the current configuration summary** in the **Backup Configuration to File** section and complete the following steps.

   Note: *The security settings on the Security page are not backed up.*

   a. Verify the settings and then click **Close**.

   b. To back up the configuration, click **Backup**.

   c. Type a name for the backup, select the location where the file will be saved, and then click **Save**.

      ✧ In Netscape Navigator, click **Save File**.

      ✧ In Microsoft Internet Explorer, select **Save this file to disk**, and then click **OK**.

Restoring and Modifying your Management Module Configuration

You can restore a saved configuration in full, or you can modify key fields in the saved configuration before restoring the configuration to your management module. Modifying the configuration file before 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 Chassis Management Module 2 also allows you to restore the default configuration or restore a configuration that was previously saved to the backplane of the Blade Server Chassis Enterprise SBCE.

The Management Module 2 and Chassis Management Module 2 have different restore procedures. They are described in the following sections.

Restoring a Management Module Configuration

To restore or modify your current 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 27.
2. In the navigation pane, click **MM Control → Configuration File**.
3. In the **Restore MM Configuration** section, click **Browse**.
4. Click the configuration file that you want; then, click **Open**. The file (including the full path) appears in the box next to **Browse**.
5. If you do not want to make changes to the configuration file, click **Restore**. A new window opens with the management module configuration information. Verify that this is the configuration that you want to restore. If it is not the correct configuration, click **Cancel**.

   If you want to make changes to the configuration file before you restore it, click **Modify and Restore** to open an editable configuration summary window. Initially, only the fields that allow changes appear. To change between this view and the complete configuration summary view, click the **Toggle View** button at the top or bottom of the window.

   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 system-management functions that you must configure after the restoration is complete. Some functions require configurations on more than one window.*
6. To proceed with restoring this file to the management module, click **Restore Configuration**. A progress indicator appears as the firmware on the Management Module 2 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 47.*
7. After you receive a confirmation that the restore process is complete, in the navigation pane, click **MM Control → Restart MM**; then, click **Restart**.
8. Click **OK** to confirm that you want to restart the Management Module 2.
9. Click **OK** to close the browser window.
10. To log in to the Management Module 2 again, start the browser, and follow your login process.

Restoring an Chassis Management Module 2 Configuration

To restore or modify your current configuration, complete the following steps. You can restore an Chassis Management Module 2 configuration only if it was previously saved to the chassis or external media, as described in "Backing up an Chassis Management Module 2 Configuration" on page 63.

1. Log in to the Chassis Management Module 2 for which you want to restore the configuration. For more information, see "Starting the Management Module Web Interface" on page 27.
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
   - Restore Configuration from Chassis
4. If you are restoring the default configuration or restoring the configuration from the chassis, click **Restore**. A new window opens with the management module configuration information. Verify that this is the configuration that you want to restore.
   - If the configuration is not correct, click **Cancel**.
   - If this is the configuration that you want to restore, click **Restore Configuration**. A progress indicator appears as the firmware on the Chassis Management Module 2 is updated. A confirmation window opens to indicate whether the update was successful.

   After the restore process is complete, go to step 6.
5. If you are restoring the configuration from a file, click **Browse** in the **Restore Configuration from File** section and complete the following steps:
   a. Click the configuration file that you want; then, click **Open**. The file (including the full path) appears in the box next to **Browse**.
   b. If you do not want to make changes to the configuration file, click **Restore**. A new window opens with the management module configuration information. Verify that this is the configuration that you want to restore. If it is not the correct configuration, click **Cancel**.

      If you want to make changes to the configuration file before you restore it, click **Modify and Restore** to open an editable configuration summary window. Initially, only the fields that allow changes appear. To change between this view and the complete configuration summary view, click the **Toggle View** button at the top or bottom of the window.

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 system-management functions that you must configure after the restoration is complete. Some functions require configurations on more than one window.*

a. To proceed with restoring this file to the Chassis Management Module 2, click **Restore Configuration**. A progress indicator appears as the firmware on the Chassis Management Module 2 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 47*.

6. After you receive a confirmation that the restore process is complete, in the navigation pane, click **MM Control → Restart MM**; then, click **Restart**.
7. Click **OK** to confirm that you want to restart the Chassis Management Module 2.
8. Click **OK** to close the browser window.
9. To log in to the Chassis Management Module 2 again, start the browser, and follow your login process.

Using the Remote Disk Feature

From the Remote Control window (see "Remote Control" on page 87), you can assign, or mount, a optical drive or diskette drive that is on the remote client computer to a blade server. By using this window, you can also specify a disk image or CD image on the remote client computer for the blade server to use.

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

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

- Microsoft Windows Server 2003*
- Microsoft Windows 2000* with Service Pack 4 or later
- Red Hat* Linux version 7.3
- SUSE* LINUX version 8.0
- Novell* NetWare 6.5

In addition, the client (remote) system must have Microsoft Windows 2000 or later and must have the Java* 1.4.1 or later Plug-in installed. The client system must also have an Intel® Pentium® III or later microprocessor operating at 700 MHz or faster (or an equivalent microprocessor).

Mounting a Disk Drive or Disk Image

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

1. Start the management module Web interface (see "Starting the Management Module Web Interface" on page 27).
2. In the navigation pane, click **Blade Tasks → Remote Control**.
3. In the **Start Remote Control** section, click **Start Remote Control**.
4. For the Chassis Management Module 2, 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 hard disk drives or images to make available for mounting from the left side of the remote disk drive selector; then, click >> to finalize the selection and move them to the right side of the remote disk drive selector. To deselect items, select them in the right side of the remote disk drive selector and then click <<.

   When you select a diskette drive or an image file and move it to the right side of the drive selector, you are given the option to save the disk image in the management module random access memory (RAM). This enables the disk image to remain mounted on the blade server so that you can access the disk image later, even if the Web interface session is terminated. Mounted drives that are not saved to the Management Module 2 will be unmounted when the remote-control window is closed.

   A maximum of one diskette drive or drive image can be stored on the Management Module 2. The size of the drive or image contents must be 1.44 MB or less.

Important: *The disk image is lost when the Management Module 2 is restarted or when the management module firmware is updated. To use the mounted disk, use the remote console function. The mounted disk appears as a USB disk drive that is attached to the server.*

6. Click **Write Protect** to prevent data from being written to the mounted drives.
7. In the right side of the remote disk drive selector, select one or more drives or images to mount; then, click **Mount Drive**.

   The mounted drive or disk image functions as a USB device that is connected to the blade server. To refresh the list of available drives on the remote client computer, click **Refresh List**.

Unmounting a Disk Drive or Disk Image

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**.

5 Management Module Web Interface

This section describes the structure and content of the management module Web interface for all management module types. It has the following information:

- Features of the management module Web interface that can be accessed by users, according to their assigned roles or authority levels (see "Web Interface Pages and User Roles")
- Descriptions of the management module Web interface pages (see "Management Module Web Interface Options" on page 73)

See Chapter 4, "Using the Management Module Web Interface," on page 23 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 2. You can use this program to perform the following tasks:

- Defining the login IDs and passwords.
- Selecting recipients for alert notification of specific events.
- Monitoring the status of the Blade Server Chassis Enterprise SBCE, blade servers, and other Blade Server Chassis Enterprise SBCE components.
- Controlling the Blade Server Chassis Enterprise SBCE, blade servers, and other Blade Server Chassis Enterprise SBCE 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 Blade Server Chassis Enterprise SBCE are viewed as USB devices by the blade server operating system.)

You also can use the management module Web interface, SNMP, and the management module command-line interface to view some of the blade server configuration settings. See the information in this chapter and the *Intel® Blade Server Chassis Enterprise SBCE Command-Line Interface Reference Guide* for more information.

Web Interface Pages and User Roles

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 Blade Server Chassis Enterprise SBCE, as follows:

- Users with the Operator role can view all information.
- Users with the Chassis Operator custom role can view information about the common Blade Server Chassis Enterprise SBCE components.
- Users with Blade Operator custom role can view information about the blade servers.
- Users with Switch Operator custom role can view information about the I/O modules.

Table 4 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 applies 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 allow a user to change the information or execute a task in that page. For example, in <xref>Table 4 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 set for each user is correct after updating management module firmware, as these definitions might change between firmware versions.*

Table 4. User Role Relationships

Page		Role required to change information or execute tasks										
		Supervisor	Chassis User Account Management	Blade Server Remote Presence	Chassis Operator	Chassis Administration	Blade Administration	I/O Module Administration	Chassis Log Administration	Chassis Configuration	Blade Configuration	I/O Module Configuration
Monitors	System Status	•	•	•		•	•	•	•	•	•	•
	Event Log (view)	•	•	•		•	•	•	•	•	•	•
	Event Log (clear)	•							•			
	LEDs	•	•	•		•	•	•	•	•	•	•
	Fuel Gauge	•	•	•		•	•	•	•	•	•	•
	Hardware VPD	•	•	•		•	•	•	•	•	•	•
	Firmware VPD	•	•	•		•	•	•	•	•	•	•
Blade Tasks	Power/Restart	•					•					
	Remote Control (remote console)	•		•								
	Remote Control (virtual media)	•		•								
	Firmware Update	•					•					
	Configuration	•									•	
	Serial over LAN	•								•	•	
I/O Module Tasks	Admin/Power/Restart	•						•				
	Configuration (see Note 1)	•										•
	Firmware Update	•						•				

Table 4. User Role Relationships

Page		Role required to change information or execute tasks										
		Supervisor	Chassis User Account Management	Blade Server Remote Presence	Chassis Operator	Chassis Administration	Blade Administration	I/O Module Administration	Chassis Log Administration	Chassis Configuration	Blade Configuration	I/O Module Configuration
MM Control	General Settings	•								•		
	Login Profiles	•	•									
	Alerts	•								•		
	Serial Port	•								•		
	Port Assignments	•								•		
	Network Interfaces	•								•		
	Network Protocols	•								•		
	Security	•								•		
	Firmware Update	•				•						
	Restore Defaults (see Note 2)	•										
	Restart MM	•				•						
Service Tools	Settings	•								•		
	Service Data	•										

Note:

- *To send ping requests to an I/O module (**Advanced Management** link in **I/O Module Tasks** → **Configuration** page), the Switch Operator role is required.*
- *For the **MM Control** → **Restore Defaults** page, both the Chassis Administration and Chassis Configuration roles are required.*

Management Module Web Interface Options

Run the management and configuration program from the management module Web interface to select the Blade Server Chassis Enterprise SBCE settings that you want to view or change.

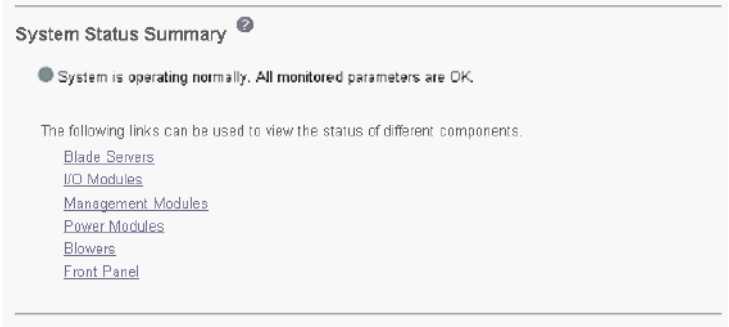
The navigation pane (on the left side of the management module Web interface window) contains navigational links that you use to manage your Blade Server Chassis Enterprise SBCE and check the status of the components (modules and blade servers). The links that are in the navigation pane are described in the following sections.

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

Monitors

Select the choices in the **Monitors** section to view the status, settings, and other information about components in your Blade Server Chassis Enterprise SBCE type.

System Status



Select **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 Blade Server Chassis Enterprise SBCE.

Blade Server Chassis Enterprise SBCE Detailed Component Status

The System Status pane provides the following detailed status information for Blade Server Chassis Enterprise SBCE components.

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

Bay	Status	Name	Pwr	Owner**		Network		WOL*	Local Control			BEM*
				KVM	MT*	Onboard	Card		Pwr	KVM	MT*	
1	●	SN#ZJ1TRL3AW112	On			Eth	--- | --- | ---	On	X	X	X	
2	●	BLADE#02	On	X	X	Eth	Fib | --- | ---	On	X	X	X	
3	●	BLADE#03	Off			Eth	--- | --- | ---	On	X	X	X	
4		*No blade present*										
5 6	●	McCarran	Off			Eth	--- | --- | ---	On	X	X	X	
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/Floppy/USB) , WOL = Wake on LAN , BEM = Blade Expansion Module , BSE = Blade Storage Expansion , PEU = Blade PCI I/O Expansion

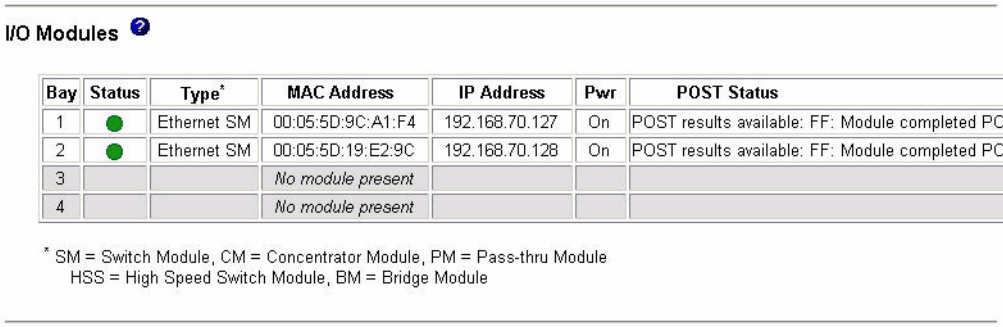
** You can change the KVM and Media Tray ownership on the Remote Control panel (under Blade Tasks).

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 bad status for the blade server. Click the icon for more detailed status information.
- **Name** - The name of the blade server.
- **Pwr** - The power state (on or off) of the blade server.
- **Owner** - An indication of whether the blade server is the current owner of the following Blade Server Chassis Enterprise SBCE resources:
  - **KVM** - Keyboard, video, and mouse
  - **MT** - The media tray containing the removable-media drives and USB ports
  - **cKVM** - An indication of whether the blade has a concurrent KVM (cKVM) expansion card installed
- **Network** - An indication of which network interfaces are on the blade server (Onboard) and the I/O expansion options (Card). For example, an Onboard status of `Eth` indicates that the blade server has integrated Ethernet controllers on the system board and a Card status of `Fibre` indicates that the blade server has a Fibre Channel I/O expansion option installed.
- **WOL** - An indication of whether the Wake on LAN feature is currently enabled for the blade server. The Wake on LAN feature is enabled by default in blade server BIOS and cannot be disabled. The Blade Server Chassis Enterprise SBCE

Management Module 2 provides a single point of control for the Wake on LAN feature, enabling the settings to be controlled for either the entire Blade Server Chassis Enterprise SBCE or a single blade server. Wake on LAN settings that are made in the Management Module 2 override the settings in the blade server BIOS. See "Power/Restart" on page 85 for information.

- **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 the SCSI expansion unit or PCI I/O Expansion Unit, occupies the blade bay.



I/O Modules

Bay	Status	Type*	MAC Address	IP Address	Pwr	POST Status
1		Ethernet SM	00:05:5D:9C:A1:F4	192.168.70.127	On	POST results available: FF: Module completed POST
2		Ethernet SM	00:05:5D:19:E2:9C	192.168.70.128	On	POST results available: FF: Module completed POST
3			*No module present*			
4			*No module present*			

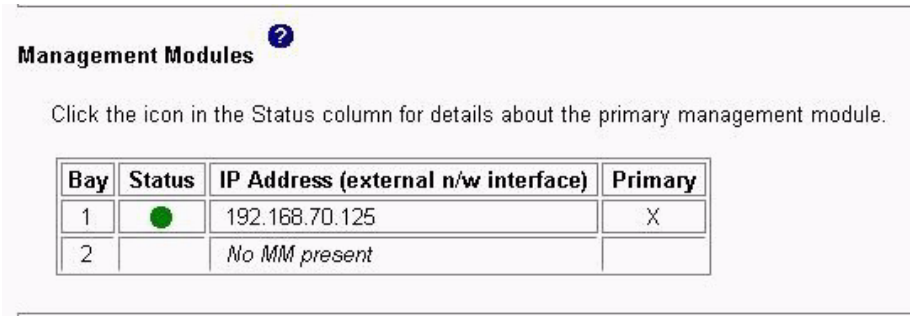
* SM = Switch Module, CM = Concentrator Module, PM = Pass-thru Module
HSS = High Speed Switch Module, BM = Bridge Module

When you click **I/O Modules**, the following information is displayed. The number of I/O module bays varies by Blade Server Chassis Enterprise SBCE type.

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

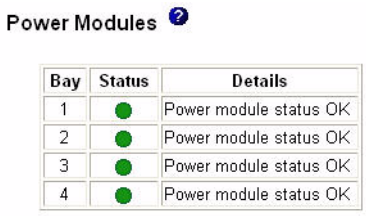
  Note: *Some types of I/O modules, such as a pass-thru module, have no MAC address nor IP address.*

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



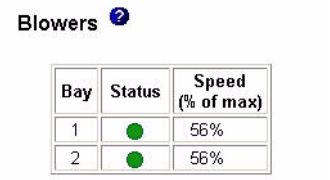
When you click **Management Module**, the following information is displayed:

- **Bay** - The number of the bay that the Management Module 2 occupies.
- **Status** - An icon that indicates good, warning, or critical status for the Management Module 2. Click the status icon for more detailed status information, such as self-test results, power-supply voltage levels, the inside temperature of the Blade Server Chassis Enterprise SBCE, and a list of users that are currently logged in to the Blade Server Chassis Enterprise SBCE. For the Chassis Management Module 2, the detailed status will also display a list of users that are logged into the management module along with their access information.
- **IP Address** - The IP address of the remote management and console connection (external Ethernet port) on the Management Module 2.
- **Primary** - An indication of which Management Module 2 is the primary, or active, management module.



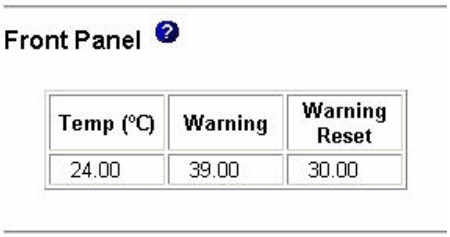
When you click **Power Modules**, the following information is displayed:

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



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

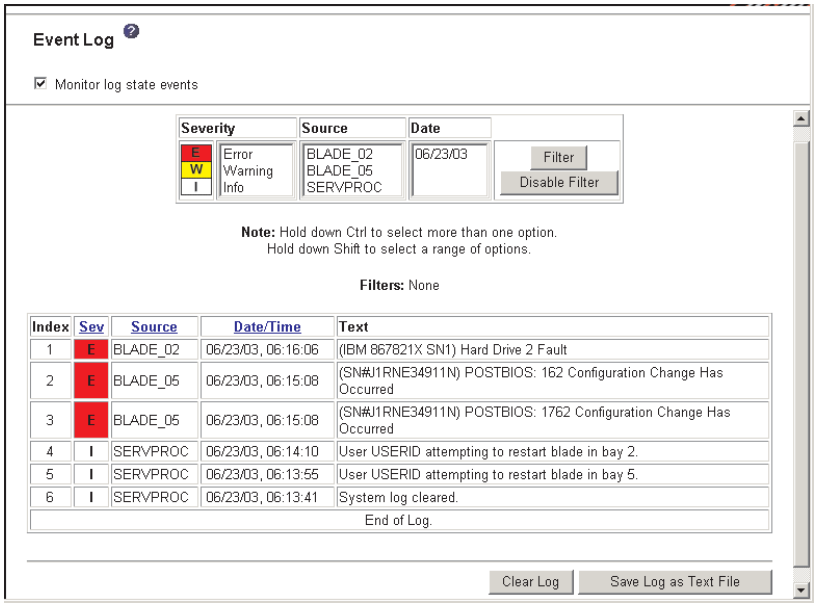
- **Bay** - The number of the bay that the blower module occupies.
- **Status** - An icon that indicates good, warning, or critical status for the blower module.
- **Speed (% of max)** - The current speed of the blower module, as a percentage of the maximum revolutions per minute (rpm). The blower speed varies with the thermal load. An entry of `Offline` indicates that the blower is not functioning.
- **Speed (RPM)** (Chassis Management Module 2 installed in a Blade Server Chassis Enterprise SBCE) - The current speed of the blower module in RPMs. The blower speed varies with the thermal load.



When you click **Front panel** the following information is displayed (front-panel temperature status is not available for all Blade Server Chassis Enterprise SBCE types):

- **Temp (C)** - The ambient temperature of the front panel, as indicated by the front-panel temperature sensor.
- **Warning** - If the ambient temperature of the front panel reaches the warning threshold, a temperature warning event occurs that is entered in the event log.
- **Warning Reset** - If the ambient temperature of the front panel exceeds the warning threshold and then drops below the warning reset threshold, the temperature warning event is cleared. An indication that the temperature warning is cleared is entered in the event log.

Event Log



Select **Event Log** to view entries that are currently stored in the management module event log. This log includes entries for events that are detected by the blade servers. The log displays the most recent entries first. Information about all remote access attempts is recorded in the event log, and the Management Module 2 sends out the applicable alerts if it is configured to do so.

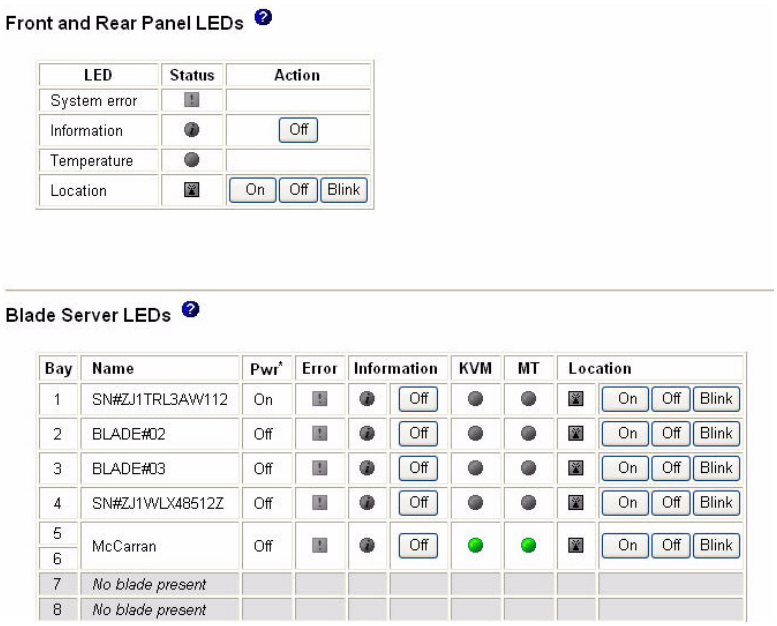
The maximum capacity of the event log is 750 entries. On the Blade Server Chassis Enterprise SBCE, when the log is 75 percent full, the Blade Server Chassis Enterprise SBCE Information LEDs are lit. When the log is full, new entries overwrite the oldest entries, and the Blade Server Chassis Enterprise SBCE Error LEDs are lit. If you do not want the Management Module 2 to monitor the state of the event log, clear the **Monitor log state events** check box at the top of the event log page.

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

LEDs

The location LEDs on the Blade Server Chassis Enterprise SBCE and their function varies based on Blade Server Chassis Enterprise SBCE.

Blade Server Chassis Enterprise SBCE LEDs



Select **LEDs** to view the state of the Blade Server Chassis Enterprise SBCE system LED panel and blade server control panel LEDs. You also can use this choice to turn off the information LED and turn on, turn off, or blink the location LED on the Blade Server Chassis Enterprise SBCE and the blade servers.

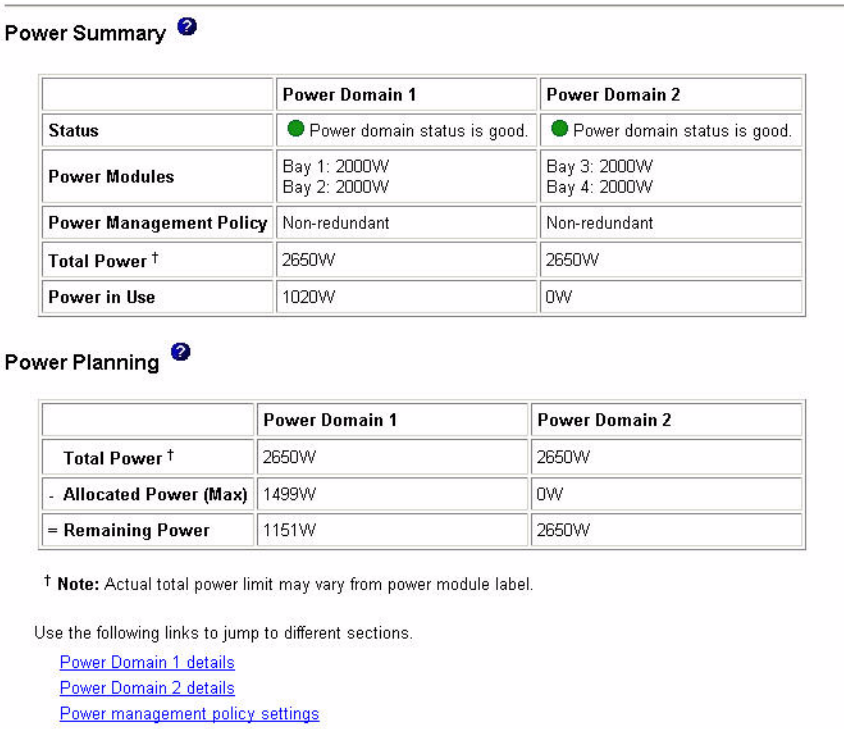
The following information is displayed:

- **Front Panel LEDs** - The state of the following LEDs on the Blade Server Chassis Enterprise SBCE system LED panel. You can change the state of the information and location LEDs.
  - System error
  - Information
  - Over temperature
  - Location

- **Blade Server LEDs** - The state of the following LEDs on the blade server control panel. You can change the state of the information and location LEDs.
  - Power
  - Error
  - Information
  - Keyboard, video, and monitor select
  - Media (optical drive, diskette drive, USB port) select
  - Location
- **Fan-pack LEDs** (Chassis Management Module 2 installed in a Blade Server Chassis Enterprise SBCE) - The state of the Error LED on each power module fan-pack.
- **Blower LEDs** (Chassis Management Module 2 installed in a Blade Server Chassis Enterprise SBCE) - The state of the Error LED on each blower.

Fuel Gauge

Select **Fuel Gauge** to view the power information, based on projected power consumption, for each power domain of the Blade Server Chassis Enterprise SBCE. Click the **Power management policy settings** link to go to the section of the **Blade Tasks → Configuration** page where you configure power management for the Blade Server Chassis Enterprise SBCE (see "Configuration" on page 90 for information).



Power Summary

	Power Domain 1	Power Domain 2
Status	Power domain status is good.	Power domain status is good.
Power Modules	Bay 1: 2000W Bay 2: 2000W	Bay 3: 2000W Bay 4: 2000W
Power Management Policy	Non-redundant	Non-redundant
Total Power †	2650W	2650W
Power in Use	1020W	0W

Power Planning

	Power Domain 1	Power Domain 2
Total Power †	2650W	2650W
- Allocated Power (Max)	1499W	0W
= Remaining Power	1151W	2650W

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

Use the following links to jump to different sections.

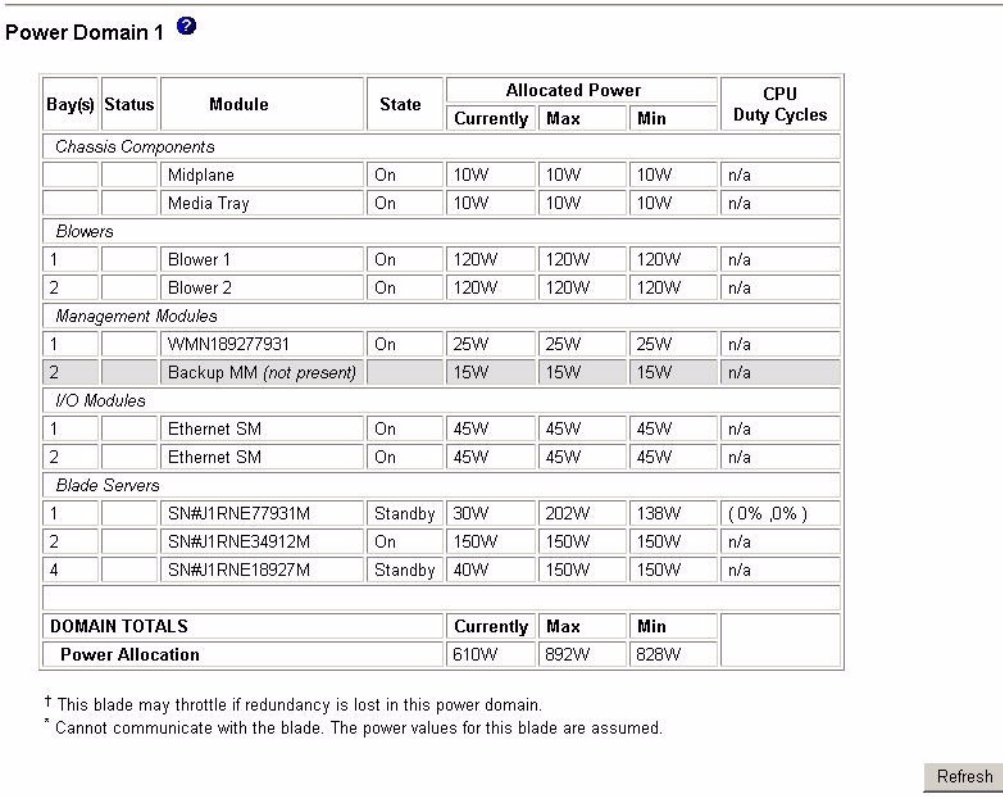
Power Domain 1 details
Power Domain 2 details
Power management policy settings

There are two power domains in the Blade Server Chassis Enterprise SBCE. Click **Power Domain 1 details** or **Power Domain 2 details** for the list of Blade Server Chassis Enterprise SBCE components in each power domain (see page 82 for information). The power-management policy settings determine how the Blade Server Chassis Enterprise SBCE reacts in each power domain to a power source failure or power module failure. The combination of the Blade Server Chassis Enterprise SBCE 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 Blade Server Chassis Enterprise SBCE **Power Summary** and Blade Server Chassis Enterprise SBCE **Power Planning** sections:

- **Status** - This field contains a color-coded icon that indicates status of the power-domains and a short status description that lists any outstanding issues related to power consumption or redundancy in each power domain.
- **Power Modules** - This field lists the power modules installed in each power domain and their rated capacity in Watts.
- **Power-Management Policy** - This field displays the power-management policy set for each power domain, defining how the power domain will react to conditions that could result in a loss of redundancy. This setting is configured on the **Blade Tasks → Configuration** page (see "Configuration" on page 90 for information)
- **Power in Use** - This field displays the current power being used in each power domain, in Watts.
- **Total Power** - This field displays the amount of power available in each power domain, in Watts. Total power is calculated by the Management Module 2, based on the rated capacities of the power modules installed in a power domain and the power-management policy that has been set for this power domain.
- **Allocated Power (Max)** - This field displays the total amount of power, in Watts, that is reserved for use by the components that are installed in a power domain. This value might include power for components that are not currently installed in the Blade Server Chassis Enterprise SBCE, such as the I/O Modules. Power is reserved for these components because the Management Module 2 pre-allocates power for some components that are normally required for Blade Server Chassis Enterprise SBCE operation. The reserved-power total might also include power for components that are installed in Blade Server Chassis Enterprise SBCE, are in a standby state, and are not turned on. These components are included in the total so that the amount of spare (unallocated) power in the power domain can be accurately calculated.
- **Remaining Power** - This field displays the amount of unallocated (spare) power in a power domain, in Watts. This value is used by the Management Module 2 when a deciding if a newly installed module should turn on. The remaining power value is calculated based on the total power and the amount of reserved power for each power domain.

Detailed Power information



Power Domain 1

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

† This blade may throttle if redundancy is lost in this power domain.
* Cannot communicate with the blade. The power values for this blade are assumed.

Refresh

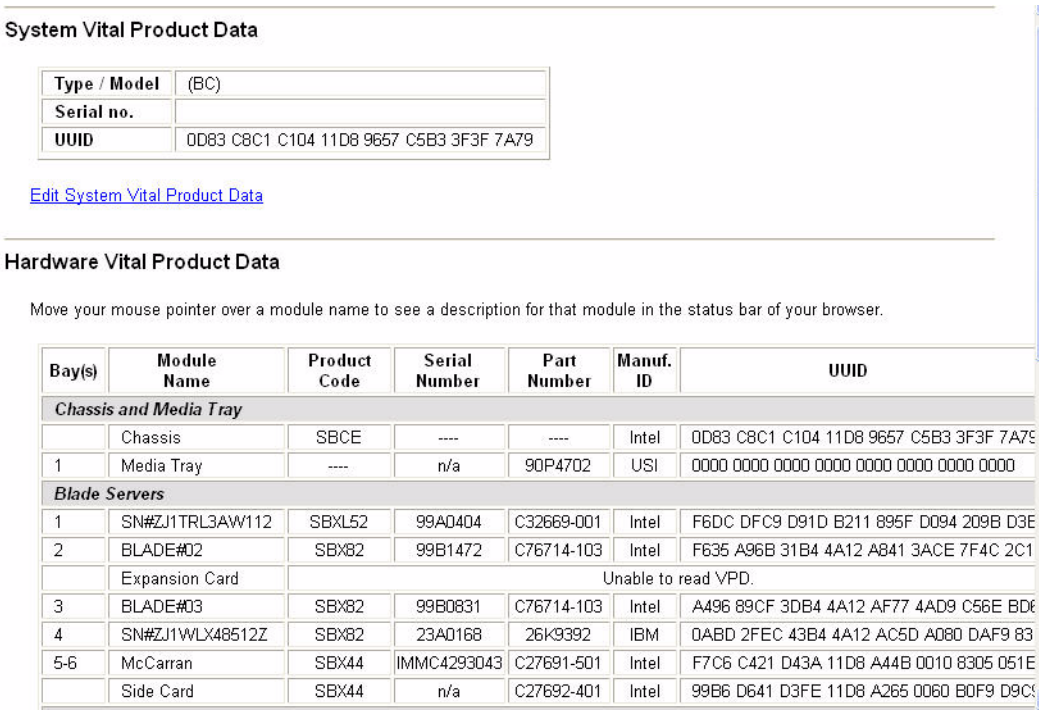
The detailed power status information for each monitored Blade Server Chassis Enterprise SBCE component is displayed in the **Power Domain details** sections of the Fuel Gauge page. The Blade Server Chassis Enterprise SBCE components that are part of each power domain are grouped by type. The status information for power domain 1 is shown. There is a separate status section for each power domain in your Blade Server Chassis Enterprise SBCE type.

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 Blade Server Chassis Enterprise SBCE component occupies. It also indicates if a blade server is able to reduce its power consumption (throttle) if power redundancy is lost.
- **Status** - This field displays an icon that indicates power-management events that are outstanding for the component. The icon indicates that a blade server will not be able to turn on because there is not enough remaining power in the power domain to support it. The icon indicates that a blade server is currently reducing its power consumption (power throttling) to maintain redundant power in a power domain.
- **Module** - This field displays the component description.
- **State** - This field displays the power state of the module (On or Standby).

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

Hardware VPD



System Vital Product Data

Type / Model	(BC)
Serial no.	
UUID	0D83 C8C1 C104 11D8 9657 C5B3 3F3F 7A79

Edit System Vital Product Data

Hardware Vital Product Data

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

Bay(s)	Module Name	Product Code	Serial Number	Part Number	Manuf. ID	UUID
Chassis and Media Tray						
	Chassis	SBCE	----	----	Intel	0D83 C8C1 C104 11D8 9657 C5B3 3F3F 7A7
1	Media Tray	----	n/a	90P4702	USI	0000 0000 0000 0000 0000 0000 0000 0000
Blade Servers						
1	SN#ZJ1TRL3AW112	SBXL52	99A0404	C32669-001	Intel	F6DC DFC9 D91D B211 895F D094 209B D3E
2	BLADE#02	SBX82	99B1472	C76714-103	Intel	F635 A96B 31B4 4A12 A841 3ACE 7F4C 2C1
	Expansion Card	Unable to read VPD.				
3	BLADE#03	SBX82	99B0831	C76714-103	Intel	A496 89CF 3DB4 4A12 AF77 4AD9 C56E BD
4	SN#ZJ1WLX48512Z	SBX82	23A0168	26K9392	IBM	0ABD 2FEC 43B4 4A12 AC5D A080 DAF9 83
5-6	McCarran	SBX44	IMMC4293043	C27691-501	Intel	F7C6 C421 D43A 11D8 A44B 0010 8305 051E
	Side Card	SBX44	n/a	C27692-401	Intel	99B6 D641 D3FE 11D8 A265 0060 B0F9 D9C

Select **Hardware VPD** to view the hardware vital product data (VPD) for the Blade Server Chassis Enterprise SBCE. When the Blade Server Chassis Enterprise SBCE is started, the Management Module 2 collects the vital product data and stores it in nonvolatile memory. The Management Module 2 then modifies the stored VPD as components are added to or removed from the Blade Server Chassis Enterprise SBCE.

The hardware VPD that is collected and stored varies by Blade Server Chassis Enterprise SBCE type. Click **Module Activity Log** to view the log of modules that have been installed in or removed from the Blade Server Chassis Enterprise SBCE. The Blade Server Chassis Enterprise SBCE **Server MAC Addresses** section at the bottom of the Hardware VPD page displays the MAC addresses of the integrated Ethernet controllers in each blade server.

Firmware VPD

Firmware Vital Product Data

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

Blade Server Firmware Vital Product Data
I/O Module Firmware Vital Product Data
Management Module Firmware Vital Product Data

Blade Server Firmware Vital Product Data

Bay(s)	Name	Firmware Type	Build ID	Released	Revision
1	SN#ZJ1TRL3AW112	BIOS	BSEO20AUS	09/27/2004	1.07
		Diagnostics	BSOT16AUS	09/21/2004	1.04
		Blade sys. mgmt. proc.	BR8T35A	n/a	35
2	BLADE#02	BIOS	BWEO21AUS	09/15/2005	1.06
		Diagnostics	BWOT10AUS	09/12/2005	1.06
		Blade sys. mgmt. proc.	BWBT22A	n/a	0
3	BLADE#03	BIOS	BWEO21AUS	09/15/2005	1.06
		Diagnostics	BWOT10AUS	09/12/2005	1.06
		Blade sys. mgmt. proc.	BWBT22A	n/a	0

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	07/15/2003	05
		Main Application 1	BRESMR4G	06/23/2005	96
2	Ethernet SM	Boot ROM	BRESMB4G	11/30/2002	04
		Main Application 1	BRESMR4G	06/23/2005	96

Management Module Firmware Vital Product Data

Bay	Name	Firmware Type	Build ID	File Name	Released	Revision
1	Intel_1	AMM firmware	BPEO14C	CNETCMUS.PKT	03-18-06	20
2		*Management Module 2 is not installed.*				

Select **Firmware VPD** to view the vital product data (VPD) for the firmware in all blade servers, I/O modules, and management modules in the Blade Server Chassis Enterprise SBCE. The firmware VPD that is collected and stored varies by Blade Server Chassis

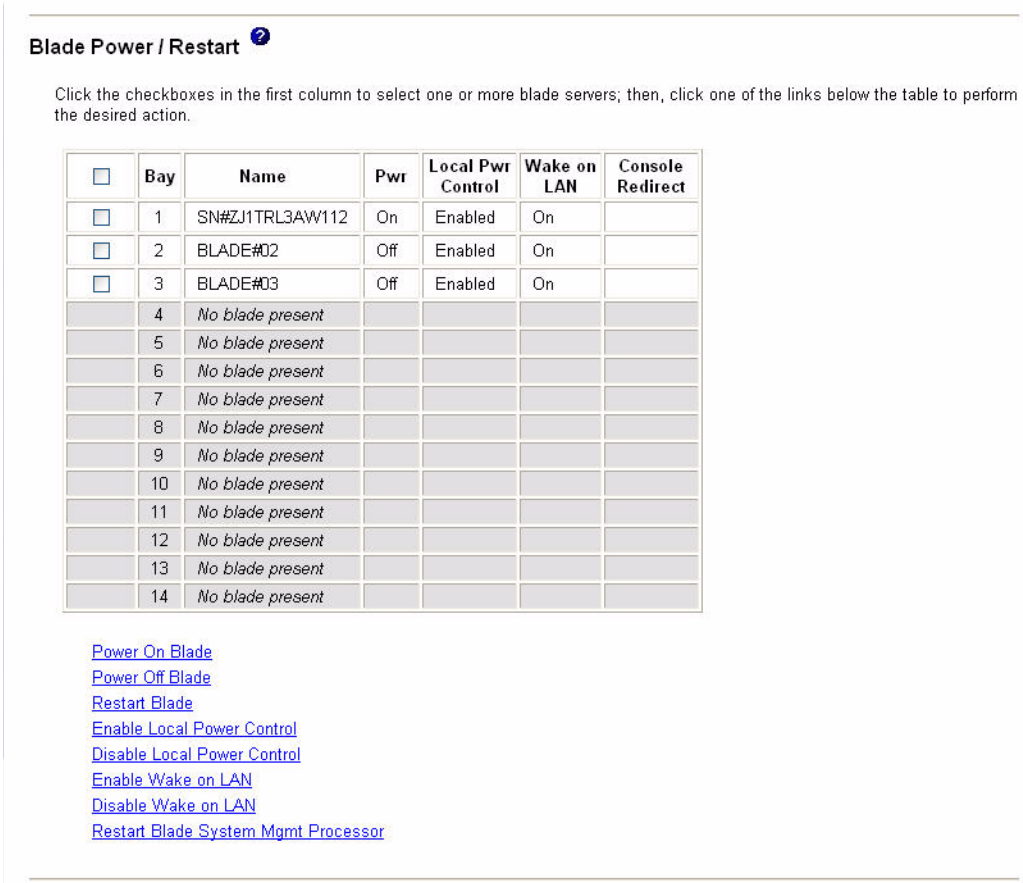
Enterprise SBCE type. For an Chassis Management Module 2 that is installed in a Blade Server Chassis Enterprise SBCE H, you can also view the VPD for blower and fan-pack firmware. The firmware VPD identifies the firmware type and provides version information such as a build ID, release date, and revision number. The VPD information varies by Blade Server Chassis Enterprise SBCE 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 VPD**, it takes up to 30 seconds to refresh and display information.)

Click **Reload VPD** to refresh the firmware VPD information for a selected blade server or for all blade servers installed in the Blade Server Chassis Enterprise SBCE.

Blade Tasks

Select the choices in the **Blade Tasks** section to view and change the settings or configurations of blade servers in the Blade Server Chassis Enterprise SBCE.

Power/Restart



Select **Power/Restart** to perform the following actions on any blade server in the Blade Server Chassis Enterprise SBCE.

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

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

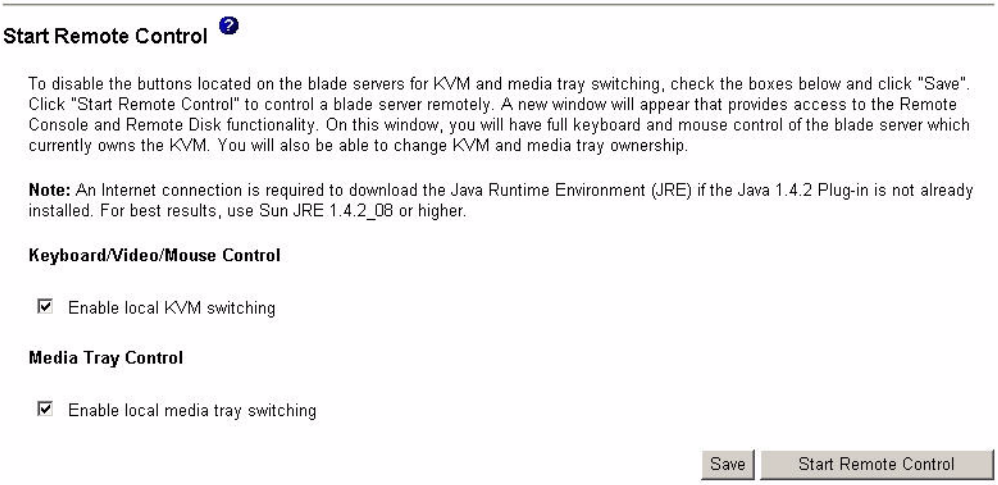
- Restart the selected blade server with non-maskable interrupt (NMI).
- Restart the selected blade server and clear all settings stored in non-volatile memory (NVRAM).
- Restart the selected blade server and run diagnostics.
- Restart the selected blade server and run diagnostics using the default boot sequence configured for the blade server.

Remote Control

The following illustration shows the Remote Control pane for the Chassis Management Module 2.

The **Firmware status** is one of the following:

- **Active** - indicates that the management module remote control application is communicating.
- **Unable to access remote control firmware** - indicates that the management module cannot use remote control.

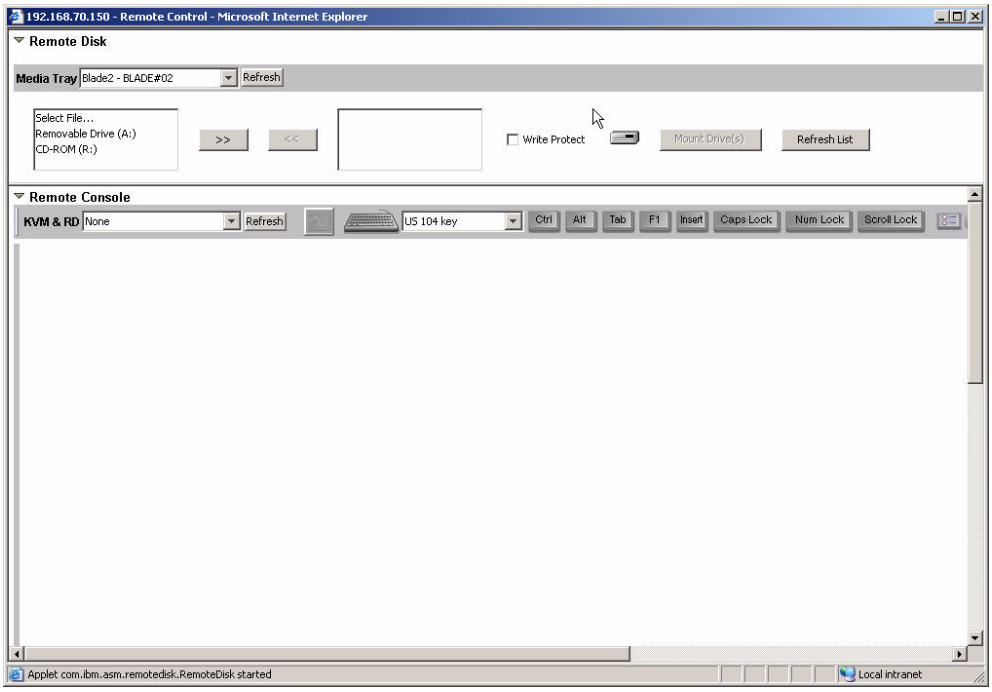


Select the **Remote Control** choice to perform the following tasks:

- View and change the current owners of the keyboard, monitor, and mouse (KVM), and of the removable-media drives and USB ports (media tray). See the *Installation and User's Guide* for your blade server type for more information about KVM and media tray switching.
- View the details of any currently active remote control session (user ID, client IP address, start time).

- Disable local switching of the KVM and of the media tray for all blade servers until they are explicitly enabled again. This prevents a local user from switching the console display to a different blade server while you are performing remote control tasks.
- Redirect a blade server console to the remote console.

The following illustration shows a remote control session for the Chassis Management Module 2.



Note: *To properly run the Java* Remote Control applet, go to the Microsoft Windows* **Start** menu and select **Java Control Panel**. Select the **Cache** tab and make sure that **Enable Caching** is not selected. Use a version of the Sun JRE that is between version 1.4.2_08 and version 1.5.x.*

On the remote console, you can perform the following tasks:

- Change the owner of the KVM and of the media tray to the blade server that you need to view. See the *Installation and User's Guide* for your blade server type for more information about KVM and media tray switching.
- Select and access the disk drives in the media tray.
- Mount a disk drive or disk image, from the computer that is acting as the remote console, onto a blade server. The mounted disk drive or disk image will appear as a USB device that is attached to the blade server. See "Using the Remote Disk Feature" on page 66 for information and instructions.
- Access files at any available network location.

- View the current blade server display.
- Control the blade server as if you were at the local console, including restarting the blade server and viewing the POST process, with full keyboard and mouse control.

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

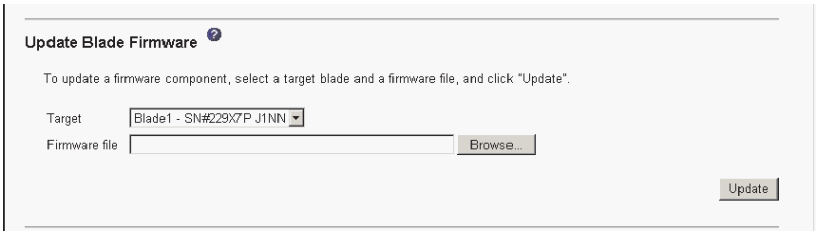
Only one remote-control session is allowed at a time. If a remote-control session is already active, you can end the current session and start a new one.

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.

When you redirect a blade server Linux X Window System session console to the remote console, the ability of the remote console applet to accurately track the location of the mouse cursor depends on the configuration of the X Window System. To configure the X Window System for accurate mouse tracking, complete the following procedure. Type the commands through the remote console or at the keyboard attached to the Blade Server Chassis Enterprise SBCE. Note that these changes require root privileges.

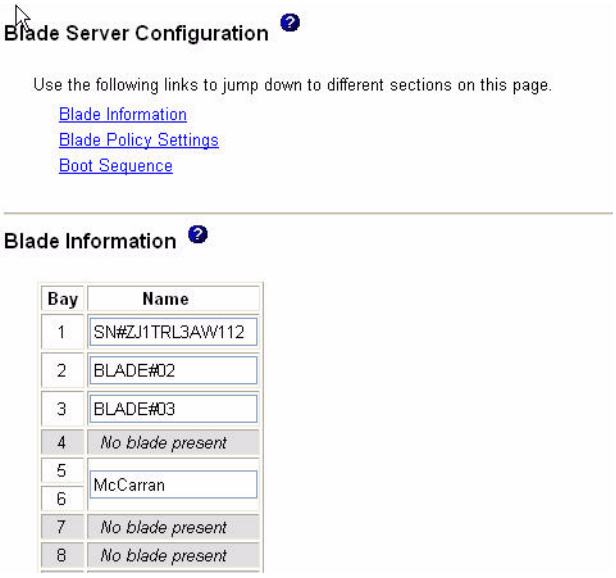
1. Enter the following commands:
   `init 3` (switch to text mode if necessary)
   `rmmod mousedev` (unload the mouse device driver)
2. Add the following statement to.xinitrc in the user's home directory:
   `xset m 1 1` (turn off mouse acceleration)
3. Add the following statement to /etc/modules.conf:
   `options mousedev xres=x yres=y` (notify the mouse device driver of the video resolution) where *x* and *y* specify the video resolution
4. Enter the following commands:
   `insmod mousedev` (reload the mouse device driver)
   `init 5` (return to GUI mode if necessary)

Firmware Update



Select **Firmware Update** to update the service processor firmware on a blade server. Select the target blade server and the firmware file to use for the update; then, click Update. Download the firmware files from http://support.intel.com/support/motherboards/server/blade.htm.

Configuration



Select the **Configuration** choice to perform the following tasks:

- Define a name for a blade server.
- Enable or disable the following items on all blade servers in the Blade Server Chassis Enterprise SBCE:
  - Local power control
  - Local KVM control
  - Local media tray control
  - The Wake on LAN feature
- Configure how each Blade Server Chassis Enterprise SBCE power domain responds if power demand in the domain is greater than the redundant power-module capacity. If this condition occurs, a single power module in the domain will not be able to meet the power needs of the domain should its companion power module fail. You select a domain power-management policy that is enforced if demand exceeds capacity when initial power is applied to the Blade Server Chassis Enterprise SBCE or when a blade server is installed in the Blade Server Chassis Enterprise SBCE. The power requirements for each component are analyzed when they initially request power. The following power-management policy options are supported:
  - Redundant with potential performance impact

    For this policy, blade servers are turned on only if the power limit calculated for the power domain, based on the selected power management policy, is not exceeded. If power module redundancy is lost, the blade servers in the power domain with microprocessors that are capable of throttling will throttle down until the power in use is less than or equal to the power available from the

remaining power module. Blade servers will power up in a throttled state in some configurations. After power redundancy is restored, the blade server microprocessors will return to their un-throttled performance levels. This option only affects the Blade Server Chassis Enterprise SBCE components that support power throttling.

— Redundant without performance impact

For this policy, new components installed in the power domain are turned on only if they can operate at their maximum power level if power redundancy in the domain is lost.

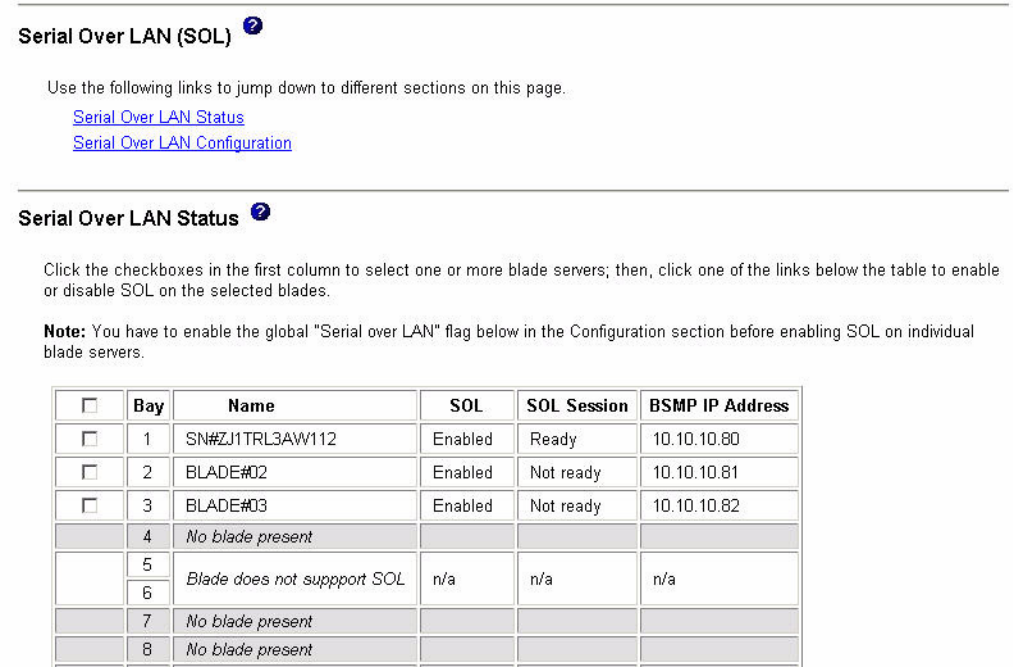
— **Non-redundant** (default setting)

For this policy, blade servers are turned on, only if the power limit calculated for the power domain, based on the selected power management policy, is not exceeded. If power module redundancy is lost, then the blade servers in the power domain with microprocessors that are capable of throttling will attempt to throttle down until the power in use is less than or equal to the power available from the remaining power module. After power redundancy is restored, the blade server microprocessors will return to their un-throttled performance levels. If blade servers are not able to reduce their power needs, power in the domain might be lost.

- Determine how the Management Module 2 responds if it detects a over-temperature condition (thermal event) on a blade server. The following acoustic mode (quiet mode) options are supported in response to thermal events:
  - — Disabled (default) - increases the blower speeds to provide additional cooling.
  - — Enabled - reduce blade server power consumption (throttle blade servers) to stay within acoustic noise limits (quiet mode). This option only affects the Blade Server Chassis Enterprise SBCE components that support power throttling.
- View or define the startup (boot) sequence for one or more blade servers. The startup sequence prioritizes the following boot-record sources for a blade server. Boot sequence choices for your Blade Server Chassis Enterprise SBCE type might include:
  - — Hard disk drives (0 through 3). The selection of hard disk drives depends on the hard disk drives that are installed in your blade server.
  - — CD-ROM (optical drive).
  - — Diskette drive (some Blade Server Chassis Enterprise SBCE types)
  - — Network - PXE. Selecting Network - PXE attempts a PXE/DHCP network startup the next time the blade server is turned on or restarted.

Note: *To use the optical drive or diskette drive (some* Blade Server Chassis Enterprise SBCE *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 supported for your* Blade Server Chassis Enterprise SBCE *type), 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 87*.

Serial Over LAN



Serial Over LAN (SOL)

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

Serial Over LAN Status
Serial Over LAN Configuration

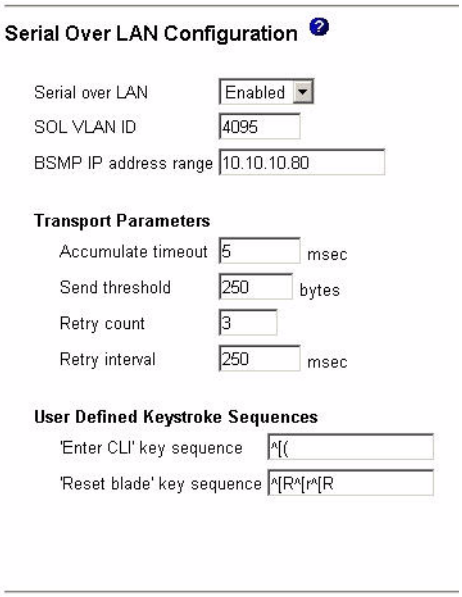
Serial Over LAN Status

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

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

	Bay	Name	SOL	SOL Session	BSMP IP Address
☐	1	SN#ZJ1TRL3AW112	Enabled	Ready	10.10.10.80
☐	2	BLADE#02	Enabled	Not ready	10.10.10.81
☐	3	BLADE#03	Enabled	Not ready	10.10.10.82
	4	*No blade present*			
	5	*Blade does not suppport SOL*	n/a	n/a	n/a
	6				
	7	*No blade present*			
	8	*No blade present*			

Select **Serial Over LAN** to monitor the SOL status for each blade server and to enable or disable SOL for each blade server, and globally for the Blade Server Chassis Enterprise SBCE. Enabling or disabling SOL globally does not affect the SOL session status for each blade server; SOL must be enabled both globally for the Blade Server Chassis Enterprise SBCE and individually for each blade server where you plan to start an SOL session. SOL is enabled globally and on the blade servers by default.



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

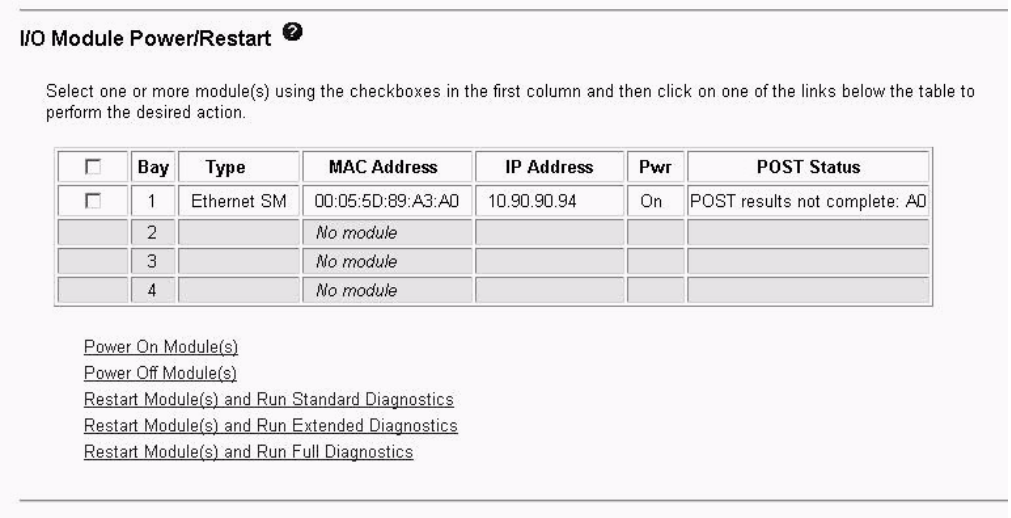
Start and run SOL sessions using the management module command-line interface. See the *Intel® Blade Server Chassis Enterprise SBCE: Management Module Command-line Interface Reference Guide* and the *Intel® Blade Server Chassis Enterprise SBCE: Serial Over LAN (SOL) Setup Guide* for more information.

I/O Module Tasks

Select the choices in the **I/O Module Tasks** section to view and change the settings or configuration on network-interface I/O modules in the Blade Server Chassis Enterprise SBCE.

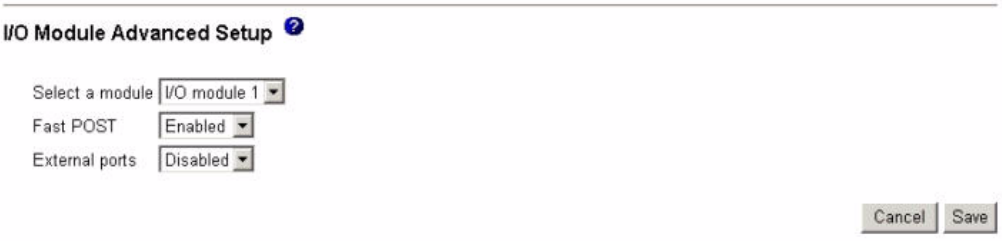
Note: *Some choices do not apply to, and are not available for, some types of I/O modules such as pass-thru modules.*

Admin/Power/Restart



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

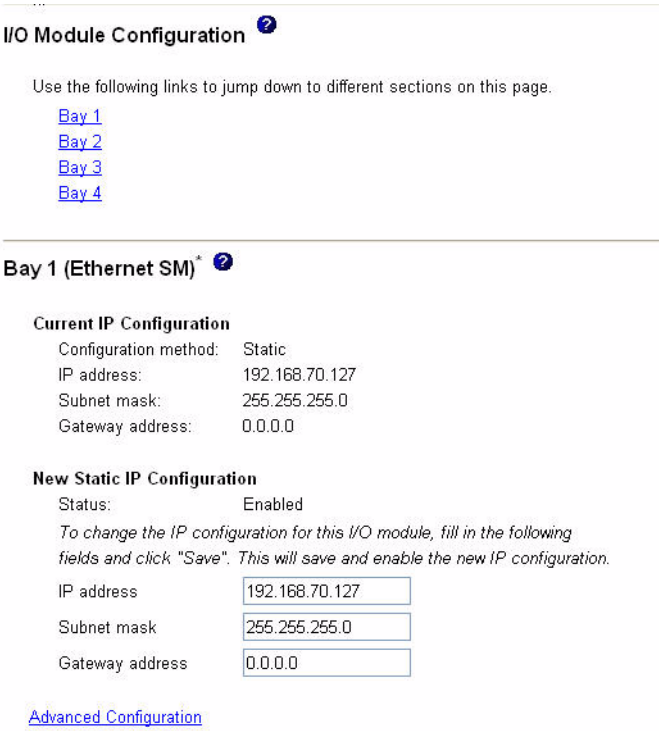
- Turn on or turn off an I/O module
- Reset an I/O module



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

- Fast POST
- External ports

Configuration



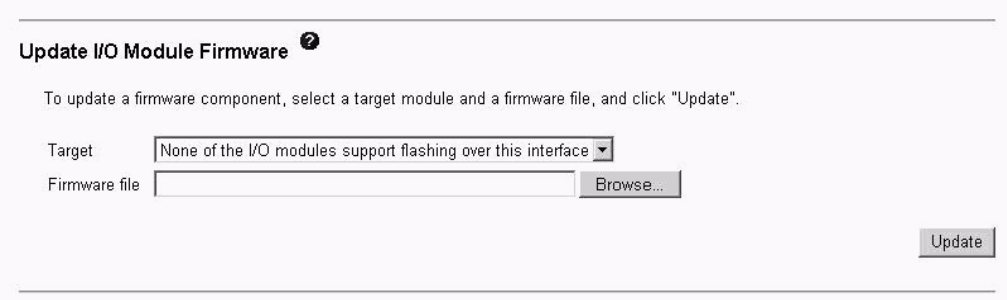
Select **Configuration** to view or change the IP configuration of the I/O modules. Select **Advanced Management** to enable external management, ping an I/O module, configure other advanced I/O module settings, return an I/O module to the default configuration, and start the configuration and management firmware that might be in an I/O module.

Note: *The initial factory-defined 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)

See the *Installation and User's Guide* for your Blade Server Chassis Enterprise SBCE type 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 *Resource CD* for your Blade Server Chassis Enterprise SBCE.

Firmware Update



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

MM Control

Select the choices in the **MM Control** section to view and change the settings or configuration on the Management Module 2 that you are logged in to (the primary management module) through the management module Web interface session. If your Blade Server Chassis Enterprise SBCE has redundant management modules, 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:

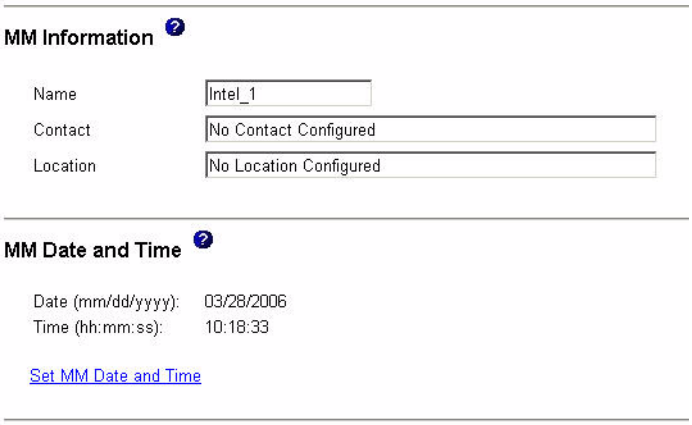
- The name of the management module
- Up to 12 login profiles for logging in to the management module
- Ports used by the management module
- How alerts are handled
- Communication settings for the advanced management module serial port
- The management module Ethernet connections for remote console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

This also includes performing the following tasks:

- Backing up and restoring the management module configuration
- Updating the management module firmware
- Restoring the default configuration
- Restarting the management module
- Switching from the primary management module that is currently active to the redundant management module (for Blade Server Chassis Enterprise SBCE units that support redundant management modules)

Note: *For Blade Server Chassis Enterprise SBCE units with a redundant management module installed, control automatically switches to the redundant management module when the primary management module fails.*

General Settings

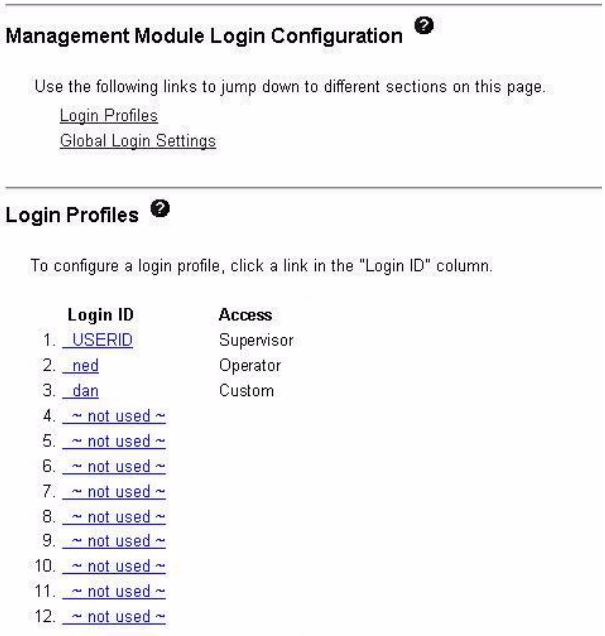


Select **General Settings** to view or change the following settings:

- The name of the Management Module 2
- The name of the contact person who is responsible for the Management Module 2
- The physical location of the Management Module 2
- The real-time clock settings in the Management Module 2

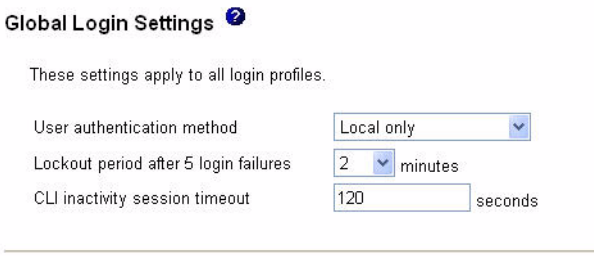
Some of the General Settings are used during SNMP and SMTP configuration. See "Configuring SNMP" on page 32 and "Configuring SMTP" on page 36 for additional information.

Login Profiles



Select **Login Profiles** to configure up to 12 login profiles for logging in to the Management Module 2; and to specify the following global login settings:

- User authentication method (local, LDAP, or both)
- Lockout period after five unsuccessful login attempts
- CLI inactivity timeout session timeout:Default timeout is 120 seconds



For each user profile, specify the following values:

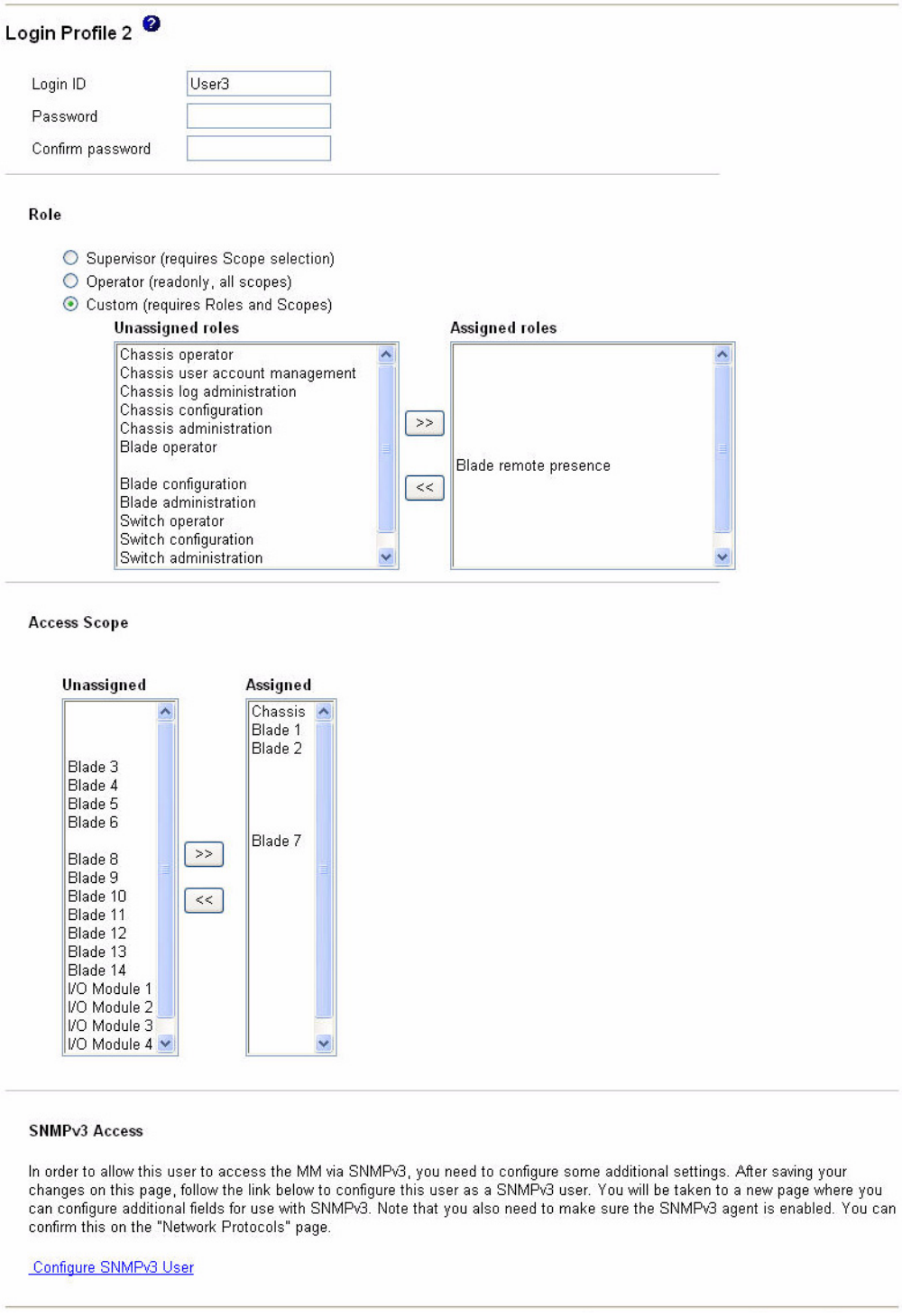
- Login ID
- Password (requires confirmation)
- Role or Authority Level (default is Operator or Read-Only)

  Defines the command areas that a user can access, based on their Access Scope. Roles or authority levels might vary based on the type of Blade Server Chassis Enterprise SBCE that you are using and the management module firmware version that is installed.
- Access Scope

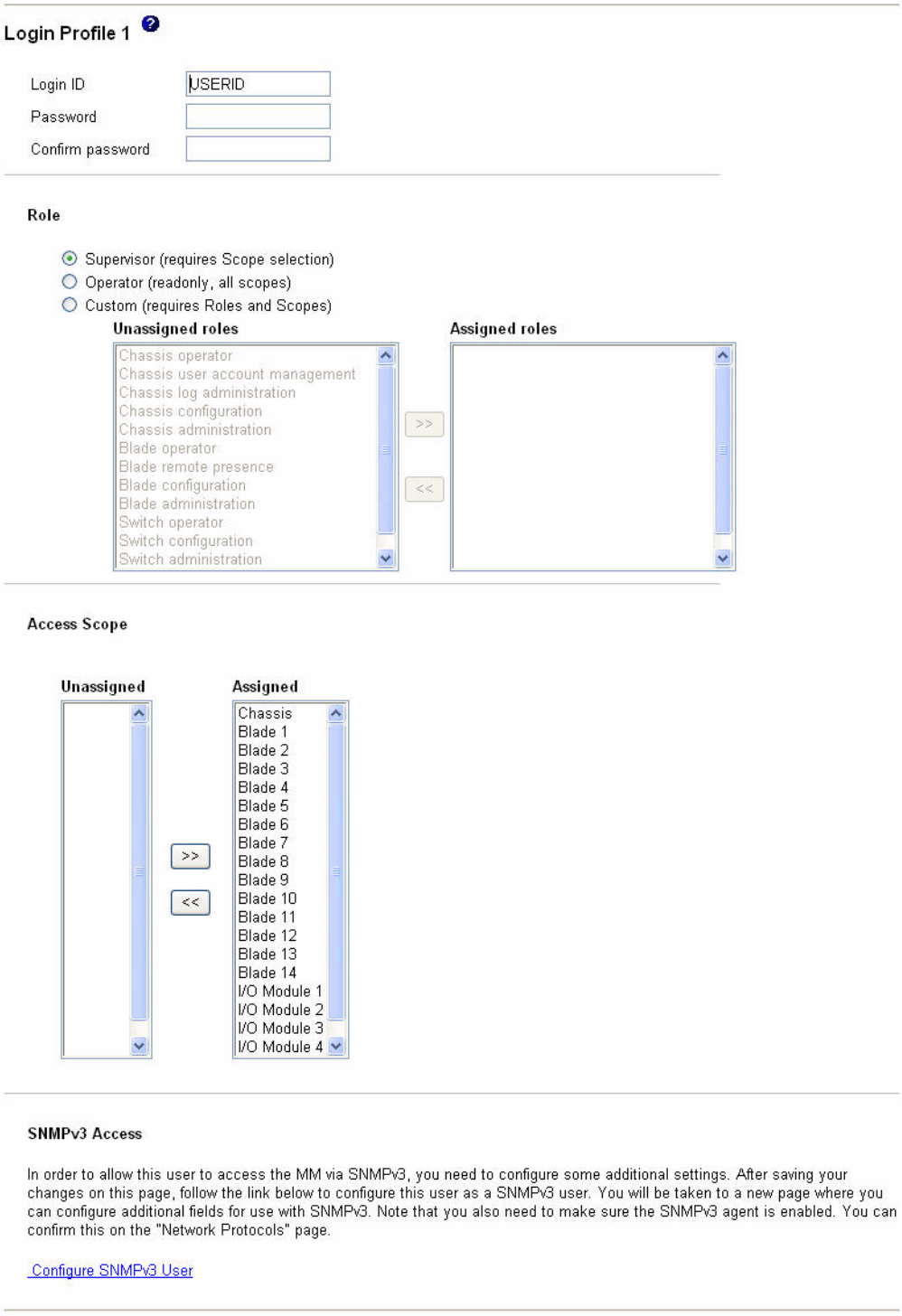
  Defines where the role or user authority defined for a user is valid.

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

The following illustration shows user profile settings for the latest version of management module firmware.


Login Profile 2
Login ID
User3
Password
Confirm password
Role
Supervisor (requires Scope selection)
Operator (readonly, all scopes)
Custom (requires Roles and Scopes)
Unassigned roles
Chassis operator
Chassis user account management
Chassis log administration
Chassis configuration
Chassis administration
Blade operator
Blade configuration
Blade administration
Switch operator
Switch configuration
Switch administration
>>
<<
Assigned roles
Blade remote presence
Access Scope
Unassigned
Blade 3
Blade 4
Blade 5
Blade 6
Blade 8
Blade 9
Blade 10
Blade 11
Blade 12
Blade 13
Blade 14
I/O Module 1
I/O Module 2
I/O Module 3
I/O Module 4
>>
<<
Assigned
Chassis
Blade 1
Blade 2
Blade 7
SNMPv3 Access
In order to allow this user to access the MM via SNMPv3, you need to configure some additional settings. After saving your changes on this page, follow the link below to configure this user as a SNMPv3 user. You will be taken to a new page where you can configure additional fields for use with SNMPv3. Note that you also need to make sure the SNMPv3 agent is enabled. You can confirm this on the "Network Protocols" page.
Configure SNMPv3 User

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



Several user roles (authority levels) are available, each giving a user write and execute access to different areas of management module and Blade Server Chassis Enterprise SBCE component function. Users with operator authority are read-only and can access management module functions for viewing only. Multiple roles can be assigned to each user using the Custom role and users with the Supervisor role have write and execute access to all functions within their assigned Access Scope.

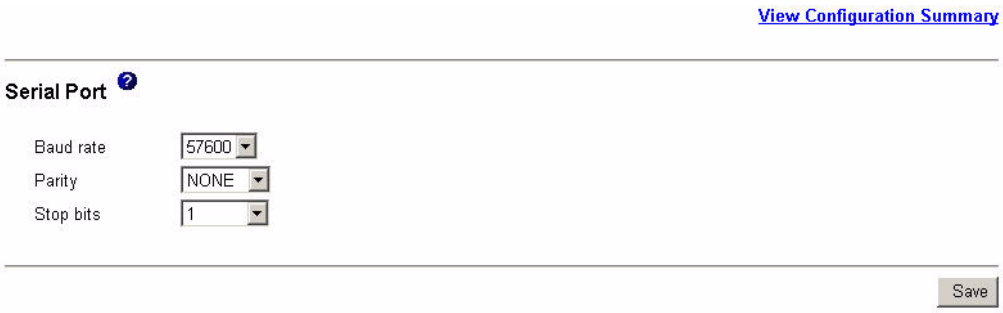
Attention: If you change the default login profile on the Management Module 2, be sure to keep a record of your login ID and password in a safe place. If you forget the management module login ID and password, you will need to call for service.

Click **Configure SNMPv3 User** to perform additional user configuration required for SNMPv3 (see "Configuring SNMP" on page 32 for instructions). Click **View Configuration Summary** to display the configuration settings for all Blade Server Chassis Enterprise SBCE users and components.

Alerts

Select **Alerts** to specify which events (from lists of critical, warning, and system alerts) are monitored, which event notifications are sent to whom, how event notifications are sent (SNMP or e-mail), whether to include the event log with the notification, and other alert parameters.

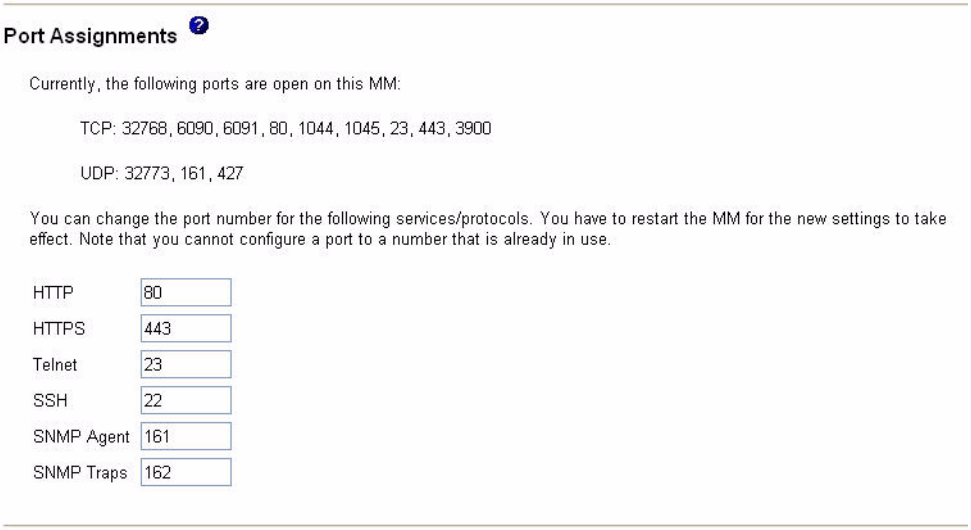
Serial Port



Select **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 made using the advanced management module serial port can only access the management module command-line interface (CLI). See the *Intel® Blade Server Chassis Enterprise SBCE: 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 Blade Server Chassis Enterprise SBCE users and components.

Port Assignments



Select **Port Assignments** to configure some of the ports that are used by the Management Module 2. Management module ports that can be configured on the Port Assignments page are listed in Table 5.

Table 5. User-configurable Management Module Ports

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

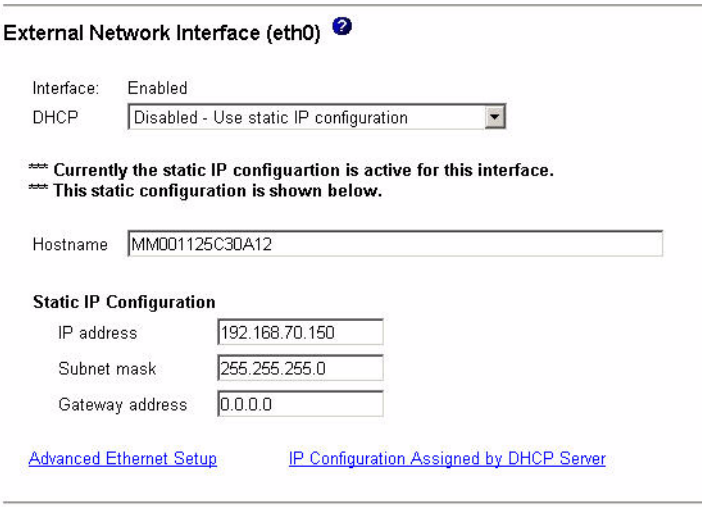
Other ports that are used by the Management Module 2 are listed in <xref>Table 6 on page 5104 These ports are fixed and cannot be modified.

Table 6. Fixed Management Module Ports

Port number (fixed)	Description
25	Port used for TCP e-mail alerts
53	Port used for the UDP Domain Name Server (DNS) resolver
68	Port used for DHCP client connection using UDP
427	Port used for the UDP Service Location Protocol (SLP) connection
1044	Port used for remote disk function
1045	Port used for persistent remote disk (disk on card)
3900	Port used for remote KVM
5900	Port used for the TCP server applet (not available for the Chassis Management Module 2)

Click **View Configuration Summary** to display the configuration settings for all Blade Server Chassis Enterprise SBCE users and components.

Network Interfaces



Select **Network Interfaces** to configure the management module Ethernet interfaces and view the TCP log (the TCP log is not available for the Chassis Management Module 2). For the Chassis Management Module 2, you can configure only the external Ethernet interface used to communicate with the remote management and console.

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 2 is not able to apply the IP address that it has in NVRAM for the I/O module, the I/O module uses whatever IP address that it has in its own NVRAM. If the two IP addresses are not the same, you might not be able to manage the I/O module anymore. The Management Module 2 cannot apply the I/O module IP address from its NVRAM under any of the following conditions:

- The Management Module 2 is restarting.
- The Management Module 2 has failed.
- The Management Module 2 has been removed from the Blade Server Chassis Enterprise SBCE.

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 2, and 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.

- When you click **External Network Interface (eth0)**, information about the interface for the remote management and console port is displayed:

  Note: *If your* Blade Server Chassis Enterprise SBCE *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 configure and use a static IP address. (The IP configuration information will be transferred to the redundant management module automatically when needed.)*

  — **Interface** - The status (Enabled or Disabled) of the Ethernet connection. The default is Enabled. (For the Chassis Management Module 2, this field is for information only and cannot be changed.)

  — **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).

  — **Hostname** - (Optional) This is the IP host name that you want to use for the Management Module 2 (maximum of 63 characters and following host-naming standards).

  — **Static IP configuration** - You must configure this information only if DHCP is disabled.

  ✧ **IP address** - The IP address for the Management Module 2 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 for 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 the **Advanced Ethernet Setup** link to view and configure the data rate, duplex mode, maximum transmission (MTU), and locally-administered MAC address for this interface. The burned-in MAC address field for the external interface is read-only.

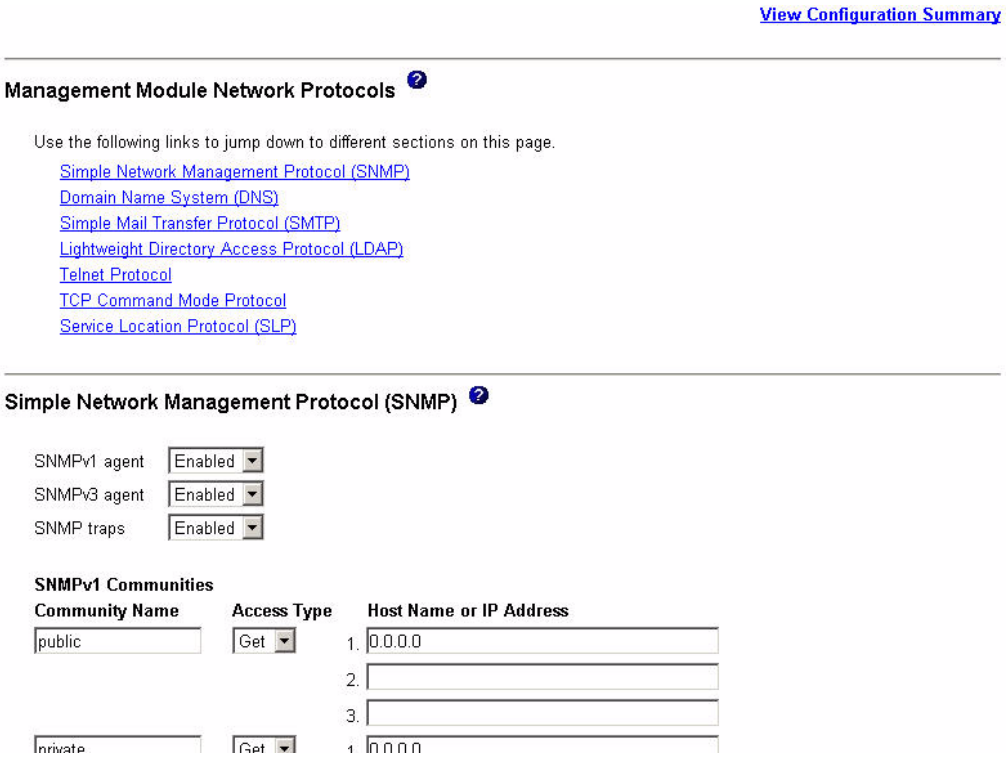
  You can enable or disable the management module uplink failover feature using the **Failover on network uplink loss** field. If the external network interface of the primary management module fails, this feature forces a failover to the redundant management module, if one is installed, after the specified network failover delay.

- When you click **Internal Network Interface (eth1)** (this selection is not available for the Chassis Management Module 2), information about the interface that communicates with the I/O modules, such as an Ethernet I/O module or the Fibre Channel I/O module, is displayed. Use it to perform the following tasks:
  - Specify the IP address to use for this interface. The internal network interface (eth1) and the external network interface (eth0) must be on the same subnet.
  - Click the **Advanced Ethernet Setup** link to view the data rate, duplex mode, maximum transmission (MTU), locally-administered MAC address, and burned-in MAC address for this interface. You can configure the locally-administered MAC address; the other fields are read-only.
- Click **TCP log** (the TCP log is not available for the Chassis Management Module 2) to view entries that are currently stored in the management module TCP log. This log contains error and warning messages that are generated by the TCP/IP code that is running on the Management Module 2; it might be used by a service representative for advanced troubleshooting. The log displays the most recent entries first.

  You can sort and filter entries in the event log.

Click **View Configuration Summary** to display the configuration settings for all Blade Server Chassis Enterprise SBCE users and components.

Network Protocols

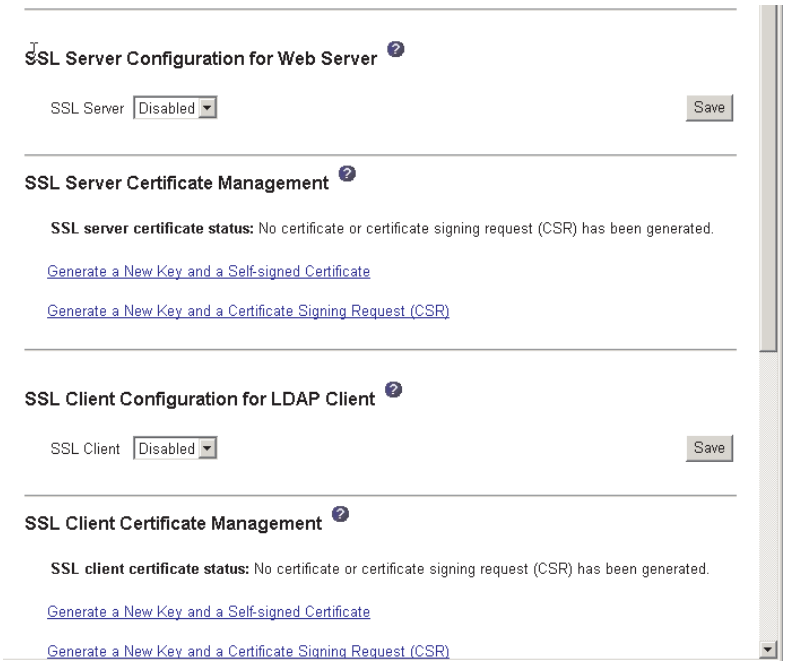


Select Network Protocols to view or change the settings for the SNMP, DNS, SMTP, LDAP, and SLP protocols. You can also enable or disable and set the timeout intervals for the Telnet and TCP interfaces.

Click **View Configuration Summary** to display the configuration settings for all Blade Server Chassis Enterprise SBCE users and components.

Some of the network protocol settings are used during SNMP, SMTP, and LDAP configuration. See "Configuring SNMP" on page 32, "Configuring SMTP" on page 36, and "Configuring LDAP" on page 36 for additional information.

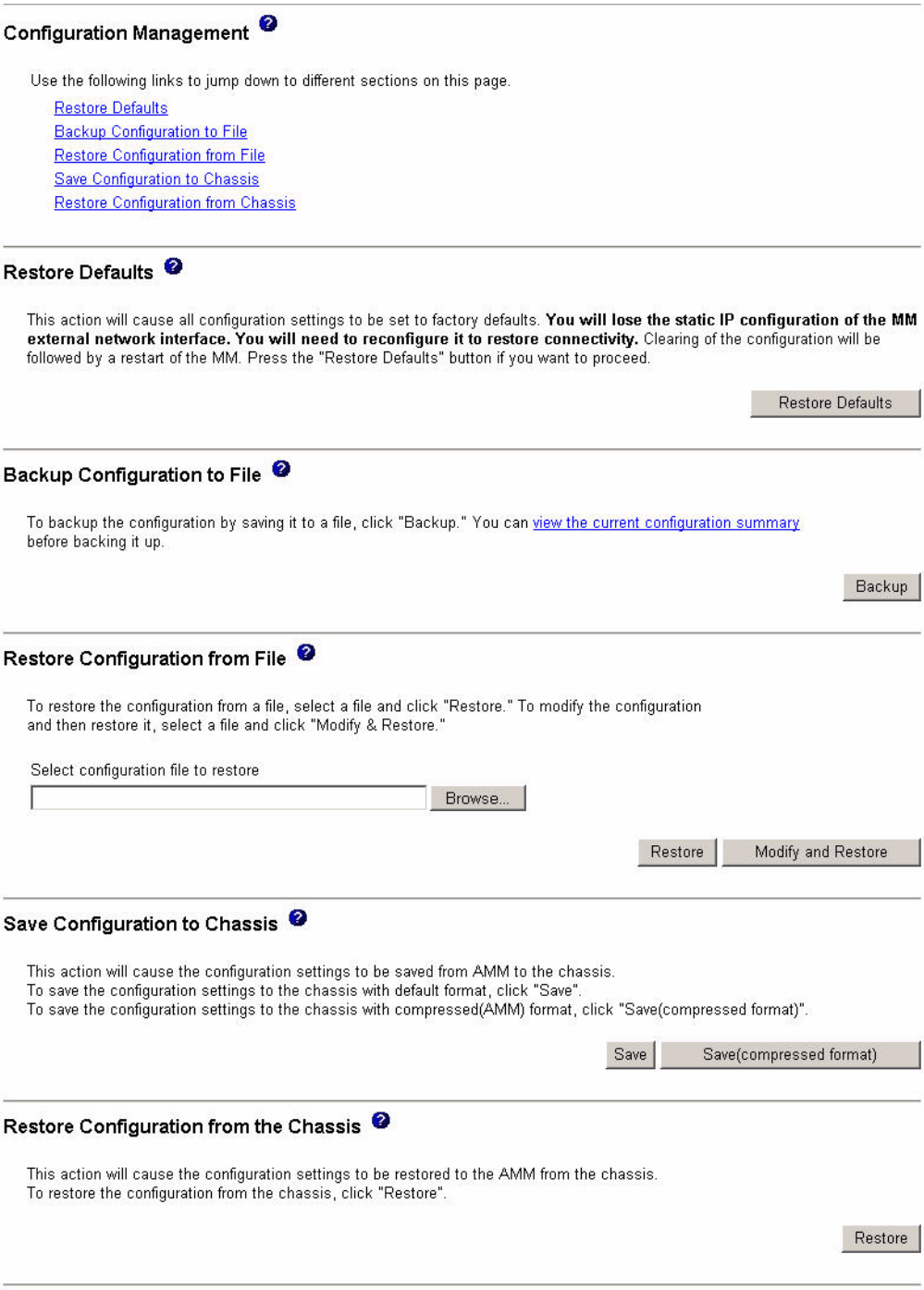
Security



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

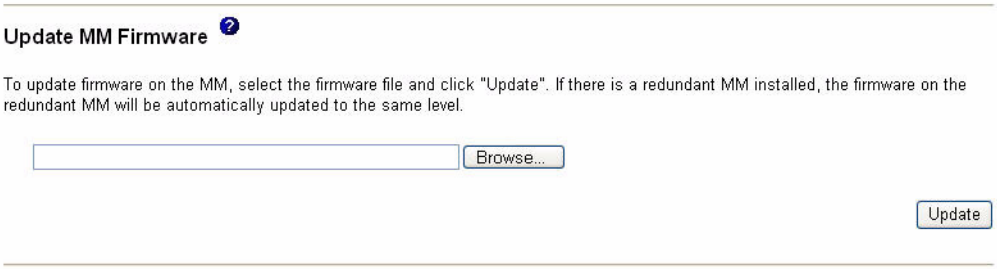
Some of the security settings are used during SSL, LDAP, and SSH configuration. See "Secure Web Server and Secure LDAP" on page 47 and "Configuring the Secure Shell Server" on page 58 for additional information.

Configuration Mgmt



Select **Configuration Mgmt** to back up or restore the management module configuration. The Chassis Management Module 2 provides several backup and restoration options. See "Using the Configuration File" on page 62 for instructions.

Firmware Update



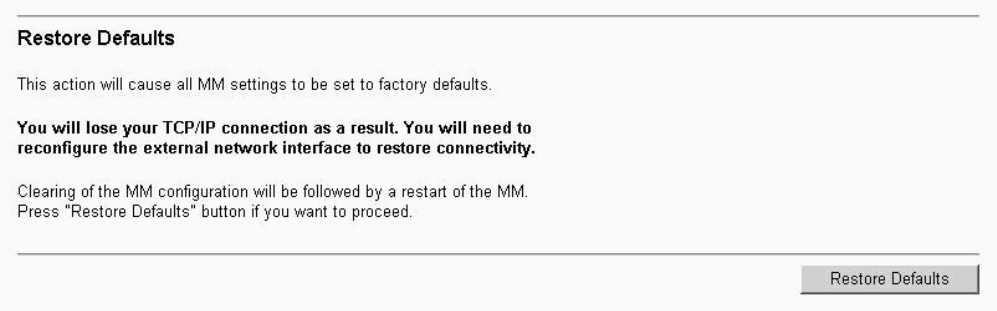
Select **Firmware Update** to update the management module firmware; if a redundant management module is installed, the firmware update will automatically be applied to both management modules. Click **Browse** to locate the firmware file that you want; then, click **Update**.

Management Module 2 firmware has a single file update. See the update instructions in the Readme file that comes with the firmware. You can obtain the firmware files from the Intel Support Web site at http://support.intel.com/.

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

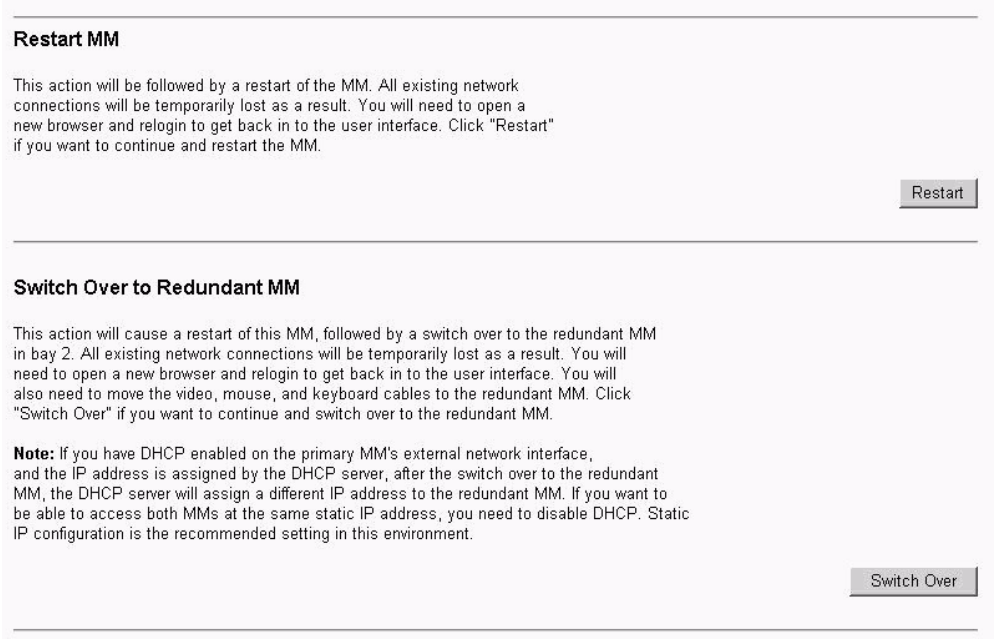
If a redundant management module is installed in a Blade Server Chassis Enterprise SBCE that previously had only one management module installed, the firmware in the new management module is updated to the firmware version that is present in the primary (already installed) management module. This update takes place when the redundant management module is installed. It does not matter if 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 redundant management module and transfer the management module configuration.

Restore Defaults



Select **Restore Defaults** to restore the factory default configuration of the Management Module 2.

Restart MM

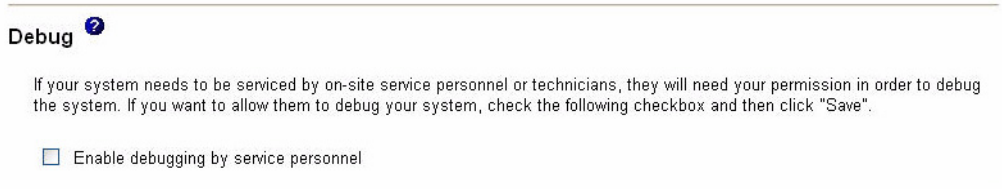


Select **Restart MM** to restart (reset) the Management Module 2. If a second management module is present, you can also select this choice to switch control to the redundant management module.

Service Tools

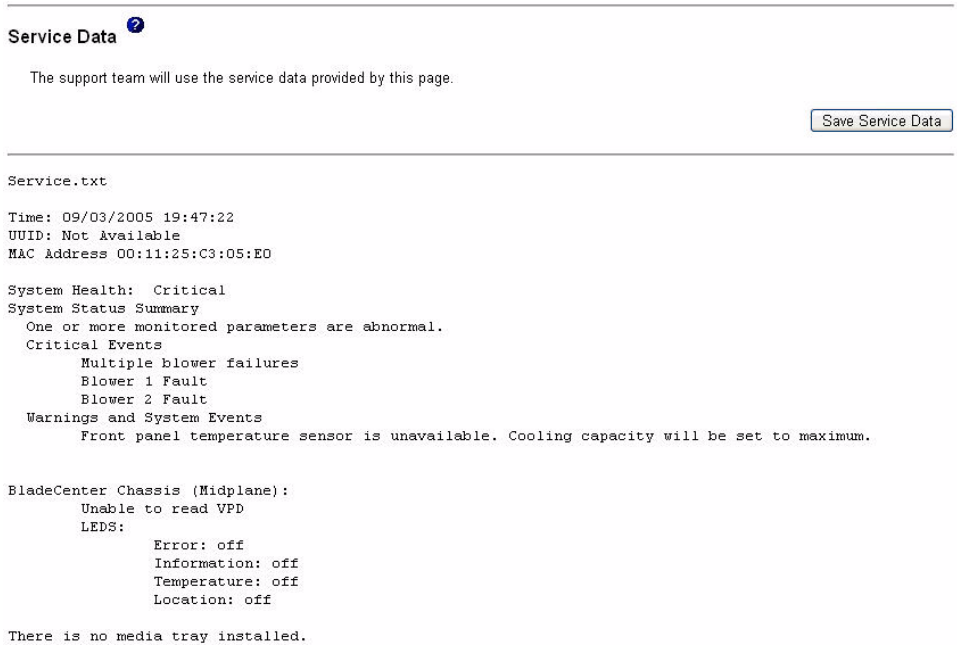
For the Chassis Management Module 2, select the choices in the **Service Tools** section to access information that might assist a technician servicing the Blade Server Chassis Enterprise SBCE.

Settings



In the **Debug** section, you can allow or restrict service access to the Blade Server Chassis Enterprise SBCE.

Service Data



In the **Service Data** section, you can view a summary of information that might be useful when servicing the Blade Server Chassis Enterprise SBCE. Click **Save Service Data** to save this information to a file on the client computer named `sdc.tgz`, for use by service personnel.

Appendix A: Getting Help

This appendix contains information about where to go for additional information about Intel and Intel products, what to do if you experience a problem with your Blade Server Chassis Enterprise SBCE and components, and whom to call for service, if necessary.

Before you Call

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

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system is turned on.
- Use the troubleshooting information in your system documentation, and use the diagnostic tools that come with your system.
- Contact your Intel Support Representative.

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

Using the Documentation

Information about your Blade Server Chassis Enterprise SBCE and pre installed software, if any, is available in the documentation that comes with your system. The documentation includes online books, README files, and help files. See the troubleshooting information in your system documentation for instructions for using the diagnostic programs. The troubleshooting information or the diagnostic programs might tell you that you need additional or updated device drivers or other software.