Intel® Server Management Module SBCECMM: Installation and User's Guide

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

Order # C61159-001

Contents

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.

Important Safety Instructions

Read all caution and safety statements in this document before performing any of the instructions. See *Intel Server Boards and Server Chassis Safety Information* on the Resource CD and/or at http:\\support.intel.com.

Wichtige Sicherheitshinweise

Lesen Sie zunächst sämtliche Warn- und Sicherheitshinweise in diesem Dokument, bevor Sie eine der Anweisungen ausführen. Beachten Sie hierzu auch die Sicherheitshinweise zu Intel-Serverplatinen und -Servergehäusen auf der Ressourcen-CD oder unter http:\\support.intel.com.

重要安全指导

在执行任何指令之前，请阅读本文档中的所有注意事项及安全声明。参见 Resource CD（资源光盘）和/或 http:\\support.intel.com 上的 *Intel Server Boards and Server Chassis Safety Information*（《Intel 服务器主板与服务器机箱安全信息》）。

Consignes de sécurité

Lisez attention toutes les consignes de sécurité et les mises en garde indiquées dans ce document avant de suivre toute instruction. Consultez *Intel Server Boards and Server Chassis Safety Information* sur le CD Resource CD ou bien rendez-vous sur le site http:\\support.intel.com.

Instrucciones de seguridad importantes

Lea todas las declaraciones de seguridad y precaución de este documento antes de realizar cualquiera de las instrucciones. Vea *Intel Server Boards and Server Chassis Safety Information* en el CD Resource y/o en http:\\support.intel.com.

v

General Safety

Follow these rules to ensure general safety:

- Observe good housekeeping in the area of the machines during and after maintenance.
- Do not perform any action that causes hazards to the customer, or that makes the equipment unsafe.
- 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 nonconductive 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.

Important: Observe the following rules when working on electrical equipment:

- Disconnect all power before performing a mechanical inspection.
- Before you start to work on the machine, unplug the power cord. or power-off the wall box that supplies power to the machine and to lock the wall box in the off position.
- 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, nongrounded power extension cables, power surges, and missing safety grounds.
- Do not touch live electrical circuits with the reflective surface of an inspection mirror. The surface is conductive; such touching can cause personal injury and machine damage.

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.

⊠⊠ **CAUTION:**
> **If your system has a module containing a lithium battery, replace it only with the same module type made by the same manufacturer. The battery contains lithium and can explode if not properly used, handled, or disposed of. Do not:**

- Throw or immerse into water
- Heat to more than 100×C (212×F)
- Repair or disassemble
- Dispose of the battery as required by local ordinances or regulations.

⊠⊠ **CAUTION:**
> **When laser products (such as CD-ROMs, DVD-ROM drives, fiber optic devices, or transmitters) are installed, note the following:**

- Do not remove the covers. Removing the covers of the laser product could result in exposure to hazardous laser radiation. There are no serviceable parts inside the device.
- Use of controls or adjustments or performance of procedures other than those specified herein might result in hazardous radiation exposure.

Danger: DANGER

> **Danger: Some laser products contain an embedded Class 3A or Class 3B laser diode. Note the following:**
>
> **Danger: Laser radiation when open. Do not stare into the beam, do not view directly with optical instruments, and avoid direct exposure to the beam.**

⊗⊗ **CAUTION:**
> **Hazardous energy is present when the blade is connected to the power source. Always replace the blade cover before installing the blade.**

Regulatory specifications and disclaimers

Safety compliance

USA:	UL 60950 - 3rd Edition/CSA 22.2. No. 60950
Canada:	cUL certified - 3rd Edition/CSA 22.2. No. 60950- for Canada (product bears the single cUL mark for U.S. and Canada)
Europe:	Low Voltage Directive, 73/23/EEC UL/CB to EN60950 3rd Edition
International:	UL/CB to IEC 60950 3rd Edition UL/CB - EN60 950 3rd Edition UL/CB - EMKO-TSE (74-SEC) 207/94
Australia/New Zealand:	CB Report to IEC 60950, 3rd Edition 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
Taiwan:	BSMI Approval
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:

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

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.

BSMI (Taiwan): The BSMI Certification number and the following warning is located on the product safety label which is located visibly on the external chassis.

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

RRL Korea:

기 종 별	사용자 안내문
A급 기기	이 기기는 업무용으로 전자파 적합등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며 만약 잘못판매 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.	

1 Introducing the Intel® Server Management Module SBCECMM

This Management Module Installation and User's Guide contains information about installing and configuring the management module and managing the SBCE unit and blade servers.

Your SBCE unit comes with one hot-swap management module in management bay 1. You can add a management module in management bay 2.

> Notes:

1. Only one management module will be active, or primary; the second management module, if present, provides redundancy.

2. When two management modules are installed in the SBCE unit, both management modules should always have the same level of firmware, to ensure smooth changeover from the active module to the redundant module.

Record information about the management module in the following table.

Product name	Intel Server Management Module SBCECMM
Part number	_____
Media access control (MAC) address	_____

The product name, machine type and part number are located on the identification label on the side of the Server Management Module. The media access control (MAC) address also is located on the identification label. See, "Overview of the management module," on page 3 for an illustration that shows the location of the identification label.

> ✏ **NOTE**
> The MAC address is also located on a separate label on the bottom front of the management module.

The management module functions as a service processor and a keyboard/video/mouse (KVM) multiplexor for the multiple blade servers. You configure the SBCE unit and modules through the management module, configuring such information as the switch IP addresses. The management module provides the following external connections: keyboard, mouse, and video for use by a local console, and one RJ-45 connector for a 10/100 Mbps Ethernet remote management connection.

The service processor in the management module communicates with the service processor in each blade server for such functions as:

- Blade server power-on requests
- Blade server error and event reporting
- Blade server requests for keyboard, mouse, and video
- Blade server requests for diskette drive, CD-ROM drive, and USB port

The management module also communicates with the I/O modules, power modules, blower modules, and blade servers in the SBCE unit to detect their presence or absence and any error conditions, sending alerts when required.

Related publications

This *Installation and User's Guide* provides general information about your management module, including information about getting started, first-time connection to the management module, how to configure your management module, and how to get help.

The following related documentation comes with your SBCE® unit:

- *Intel® Server Chassis SBCE Rack Installation Instructions*

  This publication contains the instructions to install your SBCE unit in a rack.

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

  This multilingual publication is provided in Portable Document Format (PDF) on the *Resource* CD. It contains translated caution and danger statements.

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

  This publication is provided in PDF on the *Resource* CD. It provides general information about your SBCE unit, including:

  — Information about features
  — How to set up, cable, and start your SBCE unit
  — How to install options in your SBCE unit
  — How to configure your SBCE unit
  — How to perform basic troubleshooting of your SBCE unit
  — How to get help

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

Notices and statements used in this book

The following types of notices and statements are used in this book:

- **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.

Overview of the management module

The following illustration shows the management module.

✏ **NOTE**
The illustrations in this document might differ slightly from your hardware.
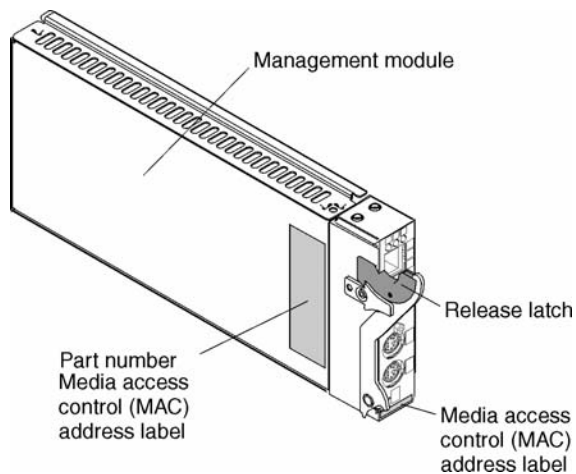
For information about the indicators and ports on the front of the management module, see "Management module controls and indicators" on page 4. For more information about the MAC address, see, "Configuring the management module for remote access," on page 8.

3

Management module controls and indicators
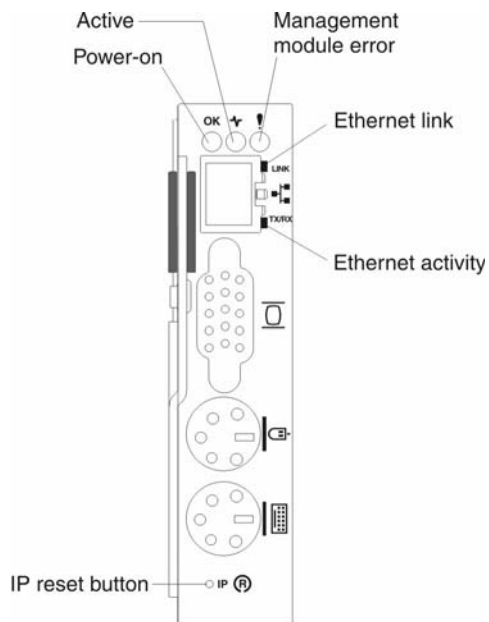
Management module LEDs: These LEDs provide status information about the management module and remote management connection. For additional information, see the Light Path Diagnostics* section in the *Intel® Server Chassis SBCE Hardware Maintenance Manual* and *Troubleshooting Guide* on the SBCE Resource CD.

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

  > ✏ **NOTE**
  > Only one management module actively controls the SBCE unit. If there are two management modules installed in the SBCE unit, this LED is lit on only one.

- **Management module error:** When this amber LED is lit, it indicates that an error has been detected somewhere on this management module. When this indicator is lit, the system error LED on the SBCE system LED panel is also lit.
- Ethernet link: When this green LED is lit, there is an active connection through the port to the network.
- **Ethernet activity:** When this green LED is flashing, it indicates that there is activity through the port over the network link.

Management module IP reset button: Do not press this button unless you intend to erase your configured IP addresses for the management module and lose connection with the remote management station, the I/O modules, and the blade servers. If you press this button, you will need to reconfigure the management module settings.

Press this recessed button to reset the IP configuration of the management module network interfaces (Ethernet 1, Ethernet 2, gateway address, and so forth) to the factory defaults and then restart the management module.

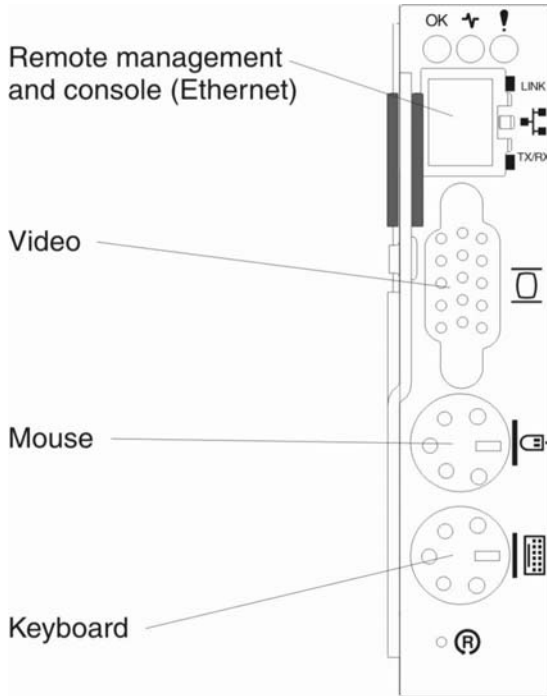Use a straightened paper clip to press the button.

Management module input/output connectors

The management module has the following I/O connectors:

- One video
- One PS/2 keyboard
- One PS/2 mouse
- One 10/100 Mbps Ethernet for remote console and management

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

✏ **NOTE**

See the *Intel® Server Management Module SBCECMM Installation Guide* for information on enabling two management modules.

Video connector

Your SBCECMM contains one standard video connector. The integrated video controller on each blade server is compatible with SVGA and VGA and communicates through this video port.
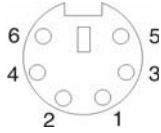
Use this connector to connect a video monitor to the SBCE unit.
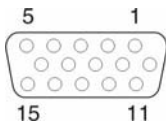
Keyboard connector

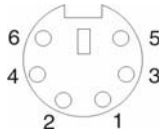Your SBCECMM contains one PS/2-style keyboard connector.

Use this connector to connect a PS/2 keyboard to the SBCE unit.

Mouse connector

Your SBCECMM contains one PS/2-style mouse connector.

Use this connector to connect a PS/2 mouse to the SBCE unit.

Remote console and management Ethernet connector

Your SBCECMM contains one 10/100 Mb Ethernet connector that provides the remote connection to the network management station on the network.

Use this port for remote console and management.

The network management station, through this port, can access control functions running in the service processor on each blade server or within each I/O module. However, it cannot use this port to communicate with application programs running in the blade servers. The network management station must direct those communications through a network connected to the external ports in the I/O modules in the SBCE unit.

The following illustration shows the Ethernet connector that is on the management module.
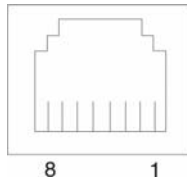
2 Installing and removing a management module

The following illustration shows the management-module bay locations.
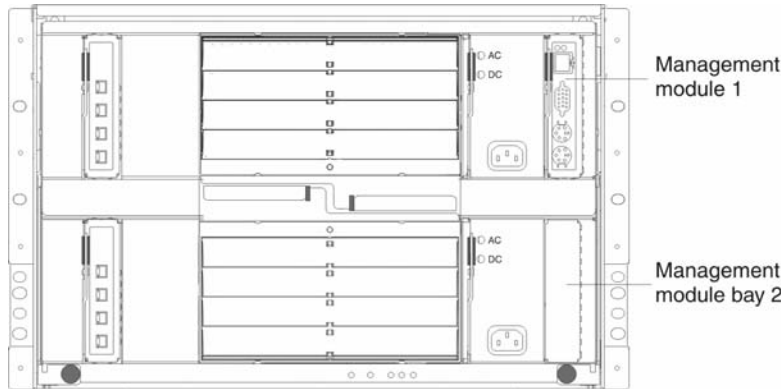
Attention: To maintain proper system cooling, each module bay must contain either a module or a filler module; each blade bay must contain either a blade or a filler blade.

Installation guidelines

Before you begin to install the management module in your SBCE unit, read the following information:

- Become familiar with the safety and handling guidelines specified under "Safety and regulatory information" on page v and "Handling electrostatic discharge-sensitive devices" on page vii and read the safety information included on the Resource CD.
- The green color on components and labels in your SBCE unit identifies hot-swap/hot-plug components. You can install or remove hot-swap modules and, with some restrictions, hot-swap blade servers while the SBCE unit is running. For complete details about installing or removing a management module, see the detailed information in this chapter.
- The blue color on components and labels identifies touch points where you can grip a component, move a latch, and so on.

  You do not need to disconnect the SBCE unit from power to install or replace any of the hot-swap modules on the rear of the SBCE unit. You need to shut down the operating system and turn off a hot-swap blade server on the front of the SBCE unit before removing the blade server, but you do not need to shut down the SBCE unit itself.

System reliability considerations

Attention: To help ensure proper SBCE cooling and system reliability, make sure that:

- Each of the module bays on the rear of the SBCE unit has either a module or filler module installed.
- Each of the blade bays on the front of the SBCE unit has either a blade server or filler blade installed.
- Each of the drive bays in a blade server storage expansion option has either a hot-swap drive or a filler panel installed.
- A removed hot-swap module, blade server, or drive is replaced within 1 minute of removal.
- Cables for the option modules are routed according to the illustrations and instructions in this document.
- A failed blower is replaced as soon as possible, to restore cooling redundancy.

7

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

Handling static-sensitive devices

Attention: Static electricity can damage electronic devices and your SBCE unit. 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, observe the following precautions:

- 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 SBCE chassis or any unpainted surface on any other grounded rack component for at least two seconds. (This drains static electricity from the package and from your body.).
- Remove the device from its package and install it directly into your SBCE unit without setting it down. If it is necessary to set down the device, put it back into its static-protective package. Do not place the device on your SBCE chassis or on a metal surface.
- Take additional care when handling devices during cold weather. Heating reduces indoor humidity and increases static electricity.

Preparing for management module redundancy

Management module redundancy requires specific minimum levels of firmware. If you intend to install a second management module in the SBCE unit, you need to make sure that you have downloaded and applied the latest level of firmware.

Complete the following steps to prepare your management modules for redundancy:

1. Obtain the hardware updates and the latest firmware from your Intel Support Representative.
2. Download the latest management module firmware and use the management module Web interface to apply it to your current management module (see "Using the management and configuration program" on page 48 for instructions about logging in to the Web interface).

   ✏ **NOTE**

   Refer to the Intel Server Management Module SBCECMM User's Guide detailed firmware update procedures.

   a. In the MM Control section in the navigation pane, click **Firmware Update**.

   b. Click **Browse** to locate the firmware file you downloaded; then, click **Update**. Follow the instructions on the screen

3. Install the second management module in the available management-module bay (see "Installing a management module" on page 9 for instructions).
4. Wait approximately 2 minutes while the primary management module transfers configuration information to the second management module.
5. Update the firmware on the second management module to the same level as on the primary management module by updating the firmware on the primary management module again:

   a. Log in to the management module Web interface again.

   b. In the MM Control section in the navigation pane, click **Firmware Update**.

   c. Make sure that the **Automatically update firmware on redundant MM** check box is selected.

d. Click **Browse** to locate the firmware file you downloaded; then, click **Update**. Follow the instructions on the screen.

The management modules are now prepared for redundancy.

Notes:

1. Whenever power is restored to a SBCE unit that has two functional management modules installed, the management module in bay 1 is automatically the active management module, even if the module in bay 2 was the active module before power was removed.
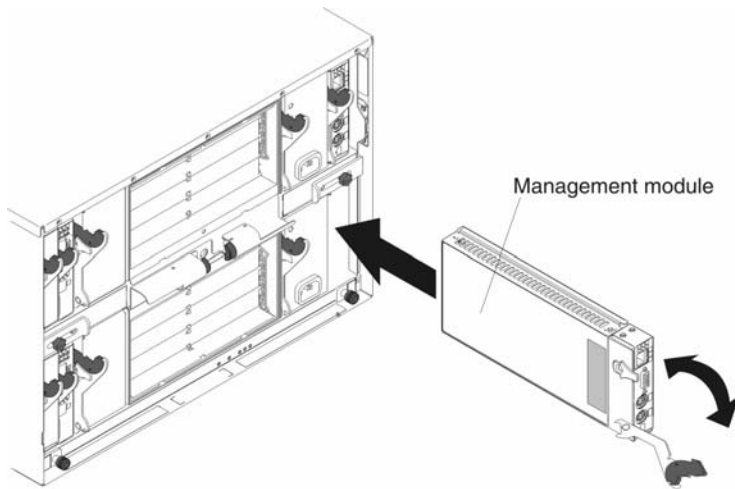
Installing a management module

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

⚠⚡ **CAUTION:**

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.

The following illustration shows how to install a management module in the rear of the SBCE unit.

Management module

Complete the following steps to install a management module.

1. Read the safety information beginning on page v and "Installation guidelines" on page 7 through "Handling static-sensitive devices" on page 8.

2. If you are installing a second management module, read "Preparing for management module redundancy" on page 8.

3. Remove the acoustic attenuation module, if one is installed, from the rear of the SBCE unit.

Acoustic module

Unlocking handle
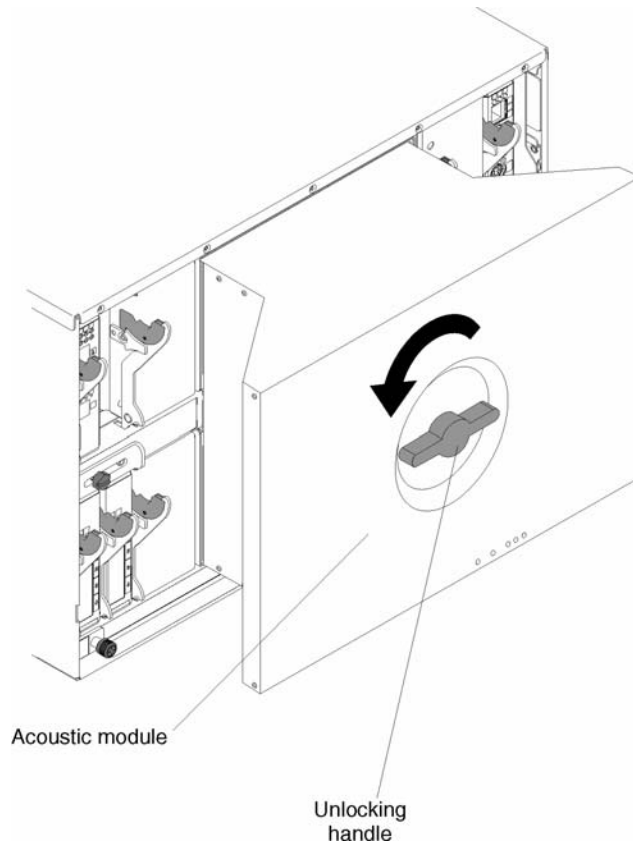
> ✏ **NOTE**
>> If you are replacing the only management module in the SBCE unit, and the management module is functional, you might want to save the configuration file to another medium before you proceed; you will be able to apply the saved configuration file to the replacement management module. See "Restoring a saved configuration file" on page 50 for information about applying a saved configuration file.

4. If you are replacing a management module, remove the current module from the bay (see "Removing a management module" on page 14). If you are adding a management module, remove the filler module from the selected management module bay and store the filler module for future use.

5. If you have not already done so, touch the static-protective package that contains the management module to an unpainted metal part of the SBCE unit or any unpainted surface on any other grounded rack component for at least 2 seconds.

6. Remove the management module from its static-protective package.

7. Ensure that the release latch on the management module is in the open position (perpendicular to the module).

8. Slide the management module into the selected management-module bay until it stops.
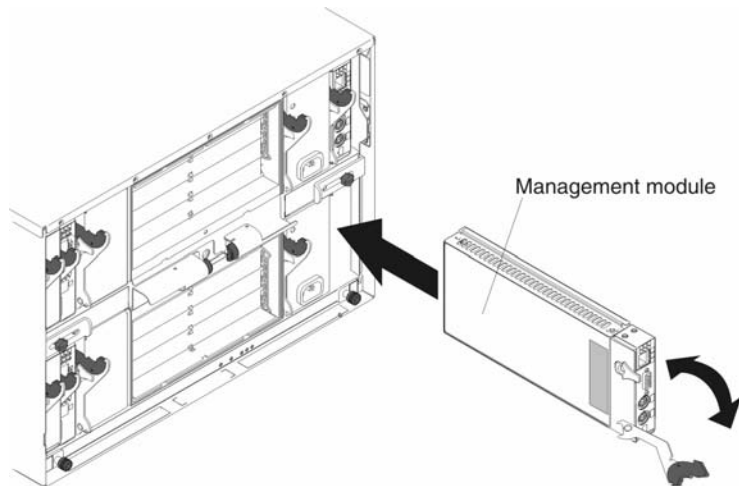
Management module

9. Push the release latch on the front of the management module to the closed position.

10. Make sure that the OK LED on each management module is lit, indicating that the management modules are operating correctly.

11. Connect the necessary cables to the management module. See "Cabling the management modules" on page 15 for more information.

12. Replace the acoustic attenuation module, if you removed it in step 3.

Acoustic module

Locking handle
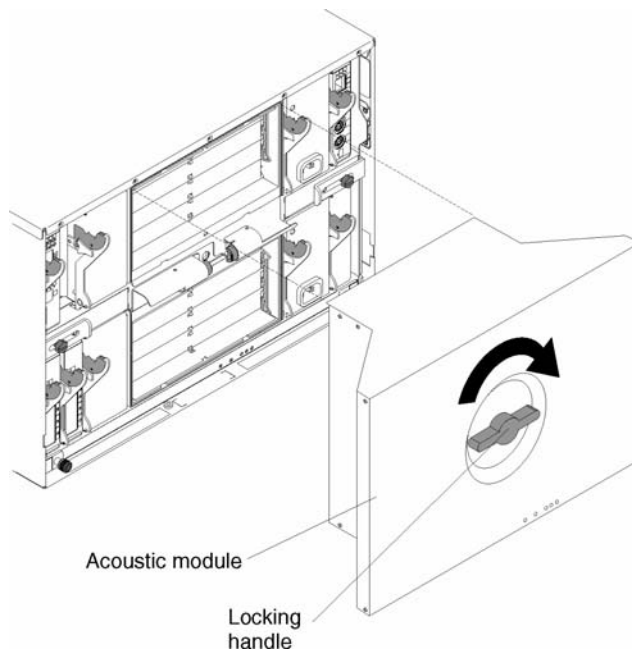
13. If this is the only management module in the SBCE unit, configure the new management module. See 3"Configuring the management module" on page 45 for more information. If this is the secondary management module, and you followed the instructions in "Preparing for management module redundancy" on page 8, no configuring is necessary. The secondary management module receives the configuration and status information automatically from the primary management module when necessary.   However, you need to apply the latest level firmware to ensure smooth changeovers; return to"Preparing for management module redundancy" on page 8 for instructions.

✏ **NOTE**
Do not initiate any management module changeover for approximately 2 minutes after installing the secondary management module; the secondary management module needs the time to receive initial status information.

Removing a management module

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

CAUTION:

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.

Complete the following steps to remove a management module.

NOTE

- These instructions assume the SBCE unit is connected to power.
- If you are removing the only management module in the SBCE unit, you might prefer to stop all management-module local and remote sessions before proceeding, to avoid unexpected termination of sessions.
- If you are replacing the only management module in the SBCE unit, and the management module is functional, you might want to save the configuration file to another medium before you proceed (under the MM Control section in the navigation pane, click **Configuration File** and follow the instructions under **Save MM Configuration**); you will be able to restore the saved configuration file to the replacement management module. See "Restoring a saved configuration file" on page 50 for more information about applying a saved configuration file.
- If you have just installed a second management module in the SBCE unit, do not remove the first (primary) management module for approximately 2 minutes; the second (secondary) management module needs the time to receive initial status information.

1. Read the safety information beginning on page v and "Installation guidelines" on page 7 through "Handling static-sensitive devices" on page 8.

2. Remove the acoustic attenuation module, if installed, from the rear of the SBCE unit (see step 3 for location).

3. Disconnect any cables from the selected management module.

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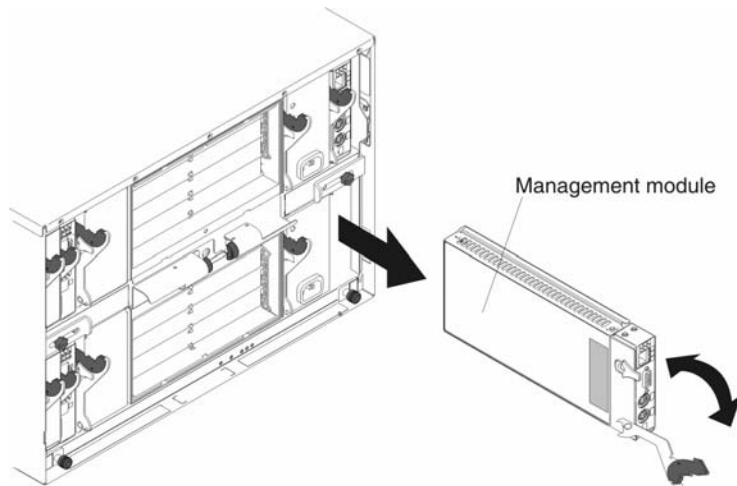
Management module

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 filler module in the bay.

6. If you placed another management module in the bay, reconnect any cables that you disconnected in step 3; then, verify that the OK LED on the management module is lit.

7. If you have not already done so, configure the replacement management module. See Chapter 3, "Configuring the SBCECMM and SBCE unit," on page 17, for more information.

8. Replace the acoustic attenuation module option, if you removed it in step 2.

Cabling the management modules

When two management modules are installed in an SBCE unit, only one management module is active; the second management module, if present, provides redundancy. The active management module is the primary module; the redundant management module is the secondary module. If the primary management module fails, or if you request a changeover through the Web interface, the secondary management module becomes active and primary.

Given this information, decide how you want the keyboard, video, and mouse at the SBCE unit to be handled when changeover occurs, and cable the management modules accordingly.

Complete the following steps to cable the management modules in an SBCE unit:

1. Connect the Ethernet port on each management module to your Ethernet network. When changeover occurs between the management modules, you will be able to communicate with the new primary management module without additional intervention, such as switching a single Ethernet cable between the management modules.

2. To be able to use the local keyboard, video, and mouse after changeover occurs, connect these devices to the management modules in one of the following ways (see "Management module input/output connectors" on page 5 for the location of each connector):

   • **Use an external keyboard, video, and mouse (KVM) switch.** Cable the keyboard, video, and mouse connectors on both management modules to the KVM switch, and connect the KVM switch to the local keyboard, monitor, and mouse. When changeover occurs, the new primary management module automatically controls the local keyboard, monitor, and mouse.

   • **Cable only to the active management module.** When management module changeover occurs, you can move the keyboard, monitor, and mouse cables to the new active management module.

15

- **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 changeover occurs.

If you always use a remote session to communicate with the blade servers in the SBCE unit, you do not need to connect a local keyboard, monitor, and mouse to either management module.

3 Configuring the SBCECMM and SBCE unit

> **Important**
>
> If the management module that you installed is the second management module in the SBCE unit, you do not configure it. The secondary management module receives the configuration and status information automatically from the primary (active) management module when necessary. The information in this chapter about configuring a management module applies to the primary or only management module in the SBCE unit.
>
> If the management module that you installed is a replacement for the only management module in the SBCE unit, and you saved the configuration file before replacing the management module, you can apply the saved configuration file to the replacement management module using the management module Web interface. See "Restoring a saved configuration file" on page 50 for information about applying a saved configuration file.

When the SBCE unit is started, it automatically configures the remote management port on the active (primary) management module, so that you can configure and manage the SBCE unit and blade servers. You configure and manage the SBCE unit remotely, through the management module, using the Web-based user interface.

If the management module that you installed is a replacement for the only management module in the SBCE unit, and you saved the configuration file before replacing the management module, you can restore the saved configuration file to the replacement management module using the management module Web interface.

✏ **NOTE**

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

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

- The external Ethernet (remote management) port on the management module. The initial management module autoconfiguration enables the network management station to connect to the management module to configure the port completely and to configure the rest of the SBCE unit.
- The internal Ethernet port on the management module for communication with the I/O modules.
- The internal Ethernet management port on each switch module. for communication with the management module. Configure this port by configuring the IP address for the switch module.

To communicate with the blade servers for such functions as deploying an operating system or application program, you also will need to configure at least one external (in-band) port on an Ethernet switch module. See the *Intel® Server Chassis SBCE Installation and User's Guide* for information about configuring external ports on Ethernet switch modules.

- Microsoft* Internet Explorer* 4.0 (with Service Pack 1), or later
- Netscape* Navigator* 4.72, or later (version 6.0 is not supported)

  Notes:

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

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

- Define the login IDs and passwords

- Select recipients for alert notification of specific events
- Monitor the status of the SBCE unit and blade servers
- Control the SBCE unit and blade servers
- Access the I/O modules to configure them
- Change the drive startup sequence in a blade server
- Set the date and time
- Remote control
- Change ownership of the keyboard, video, and mouse
- Change ownership of the CD-ROM drive, diskette drive, and USB port

You also can use the management and configuration program to view some of the blade server configuration settings. See "Using the management and configuration program" on page 20 for more information.

Setting up the remote connection

To configure and manage the SBCE unit and blade servers, you must first set up the remote connection through the Ethernet port on the management module.

Cabling the Ethernet port

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

1. Connect one end of a Category 5 or higher Ethernet cable to the Ethernet port on the management module. Connect the other end of the Ethernet cable to the network.

2. Check the Ethernet LEDs to ensure that the network connection is working. The following illustration shows the locations of the Ethernet LEDs.
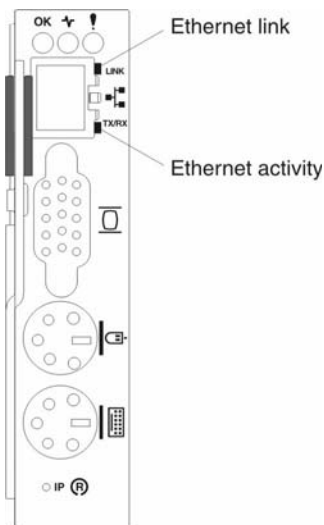
Ethernet link LED
>   When this green LED is lit, there is an active connection through the port to the network.

Ethernet activity LED
>   When this green LED is flashing, it indicates that there is activity through the port over the network link.

Configuring the management module for remote access

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

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

Either of these actions enables the Ethernet connection.

If you do not want to use the default static values, you can configure the static IP address, host name, and subnet mask for the management module through the Web interface. The default IP address is 192.168.70.125, the default subnet address is 255.255.255.0, and the default hostname is MMxxxxxxxxxxxx, where xxxxxxxxxxxx is the burned-in media access control (MAC) address. The MAC address is on a label on the management module, below the IP reset button.
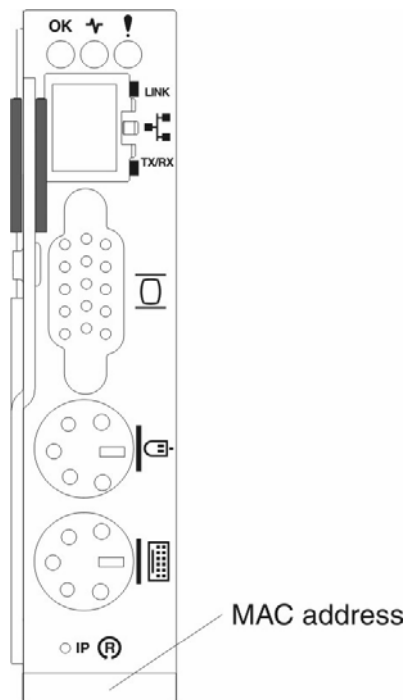
Notes:

1. All management modules are preconfigured, with the same static IP address. You can use the management module Web interface to assign a new static IP address for each SBCE unit. If DHCP is not used and you do not assign a new static IP address for each SBCE unit before attempting to communicate with management software, only one SBCE unit at a time can be added onto the network for discovery. Adding multiple units to the network without a unique IP address assignment for each SBCE unit results in IP address conflicts.

2. Pressing the IP reset button on the management module replaces the configured IP addresses for the management module with the factory default IP addresses, and loses the connection with the remote management station, the I/O modules, and the blade servers. If you press this button, you will need to reconfigure the management module settings.

19

3. 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.

Using the management and configuration program

This section provides the instructions for using the management and configuration program in the management module.

Starting the management and configuration program

Complete the following steps to start the management and configuration program:

1. Open a Web browser. In the address or URL field, type the IP address or host name defined for the management module remote connection.

   The Enter Network Password window opens.

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

   ✏ **NOTE**
       The initial user ID and password for the management module are:

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

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

Active Session from Same Client

An active session already exists for user **USERID** at **192.168.70.123**.

If you still have the browser for this active session open, use it
to access the Management Module. If you closed the browser
before logging off, you can terminate the existing session and start a
new one. To do so, select the desired inactivity timeout parameter below
and click "Start New Session".

Inactive session timeout value: no timeout ▼

Start New Session

Note: To ensure security and avoid login conflicts, always end your sessions using the "Log Off" option in the navigation frame of the main window.

The SBCECMM management and configuration window opens.

✏ **NOTE**
> The upper left corner of the management and configuration window shows the location and identity
> of the active management module.
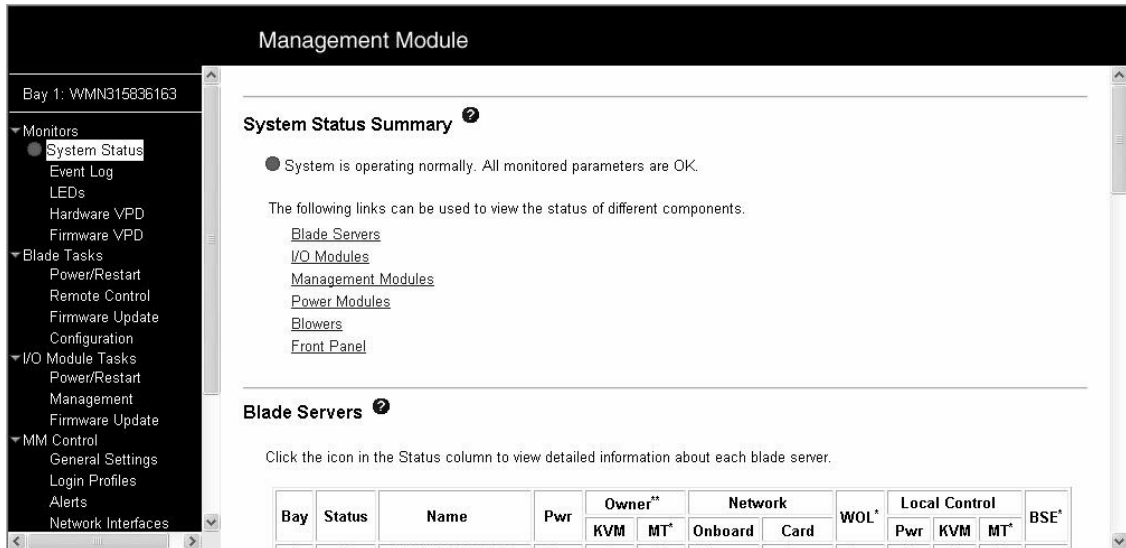
Management and configuration program options

From the management and configuration program main menu, you can select settings that you want to view or change.

The navigation pane (at the left on the management module window) contains navigational links that you use to manage your SBCE unit and check the status of the components (modules and blade servers). Descriptions of the links are as follows:

Monitors

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

System status
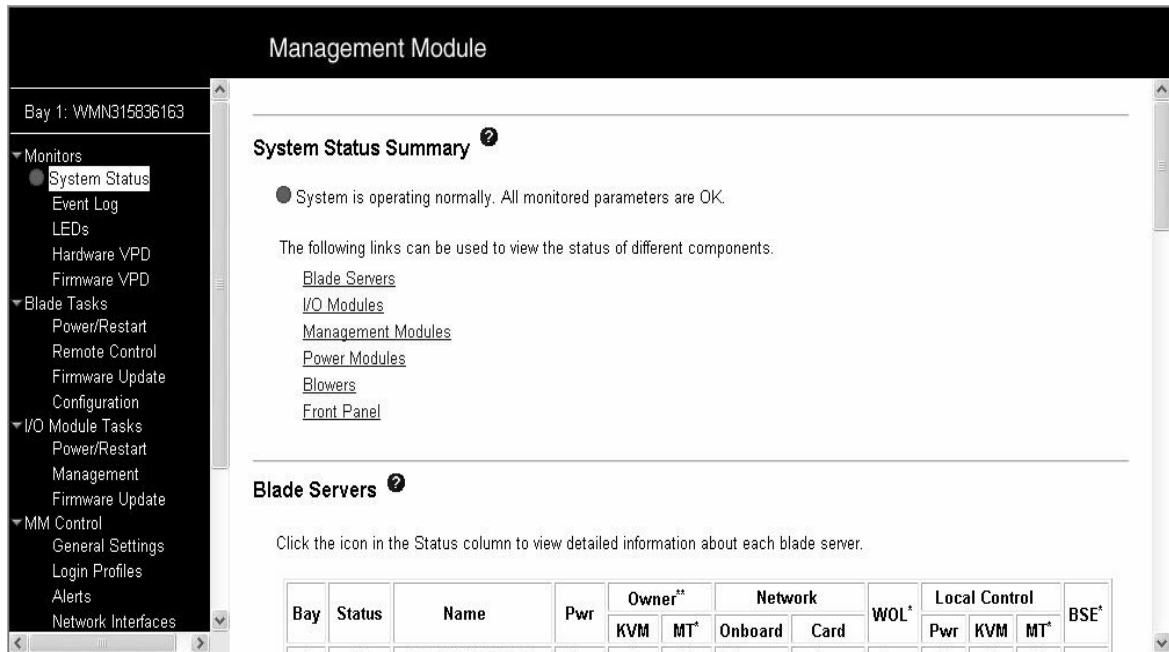
Select this choice to view the overall system status, a list of outstanding events that require immediate attention, and the overall status of each of the blade servers and I/O modules.

Blade Servers:

- **Bay -** The lowest-number bay the blade server occupies.
- **Status -** An icon that indicates good, warning, or bad for the particular 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 SBCE resources:
  — **KVM -** Keyboard, video, and mouse.
  — **MT -** The CD-ROM drive, diskette drive, and USB port.
- **Network -** An indication of which network interfaces are on the blade server (Ethernet or Fibre Channel).
- **WOL -** An indication of whether the Wake on LAN feature is currently enabled for the blade server.
- **Local Control -** an indication of whether the following options are enabled:
  — Local power control
  — Local keyboard, video, and mouse switching
  — Local CD-ROM drive, diskette drive, and USB port switching
- **BSE -** An indication of whether a SCSI expansion unit occupies the blade tray.

- **SCOD -** An indication of whether the blade server is an On Demand blade server with a Standby status. You cannot turn on an On Demand Blade server until you activate it (**Blade Tasks> On Demand)**, which changes the status from Standby to Active.

  I/O modules:
- **Bay -** The number of the bay the I/O module occupies.
- **Status -** Icon that indicates good, warning, or bad for the particular I/O module.
- **Type -** The type of I/O module in the bay, such as Ethernet or Fibre Channel.
- **MAC Address -** The media access control (MAC) address of the I/O module.
- **IP Address -** The IP address of the I/O module.
- **Power -** The power state (on or off) of the I/O module.
- **Details -** Text information about the status of the I/O module.

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

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

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

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

Event log

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

The maximum capacity of the event log is 750 entries. When the log is 75% full, the SBCE Information LEDs are lit. When the log is full, new entries overwrite the oldest entries and the Error LEDs are lit. You can sort and filter entries in the event log.

LEDs

Select this choice to view the state of the 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 SBCE unit and the blade servers.

- **Front Panel LEDs -** The state of the following LEDs on the SBCE system LED panel. You can change the state of the information and location LEDs.
  — Information
  — System error
  — 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
  — Information
  — Error
  — Location
  — Keyboard, video, and monitor select
  — Media (CD-ROM, diskette drive, USB port) select

Hardware VPD

Select this choice to view the view the hardware vital product data (VPD) for the SBCE unit. When the SBCE unit is started, the management module collects vital product data and stores it in nonvolatile memory. The management module then modifies the stored VPD as components are added to or removed from the SBCE unit. You can access this information at any time, from almost any client console. You can also view the log of modules inserted or removed from the SBCE unit.

Firmware VPD

Select this choice to view the vital product data (VPD) for the firmware in all blade servers and the I/O modules and management module in the SBCE unit. The firmware VPD identifies the firmware type, build ID, release date, and revision number. The VPD for the firmware in the management module includes the file name of the firmware components.

Blade tasks

Select the choices in this section to view and change the settings or configurations of blade servers in the SBCE unit.

Power/restart

Select this choice to perform the following actions on any blade server in the SBCE unit:

✏ **NOTE**

You cannot perform these actions on an On Demand blade server with a Standby status (identified by an X in the SCOD column). To activate an On Demand blade server, see the **On Demand** choice under **Blade Tasks** and follow the instructions.

• 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.

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

27
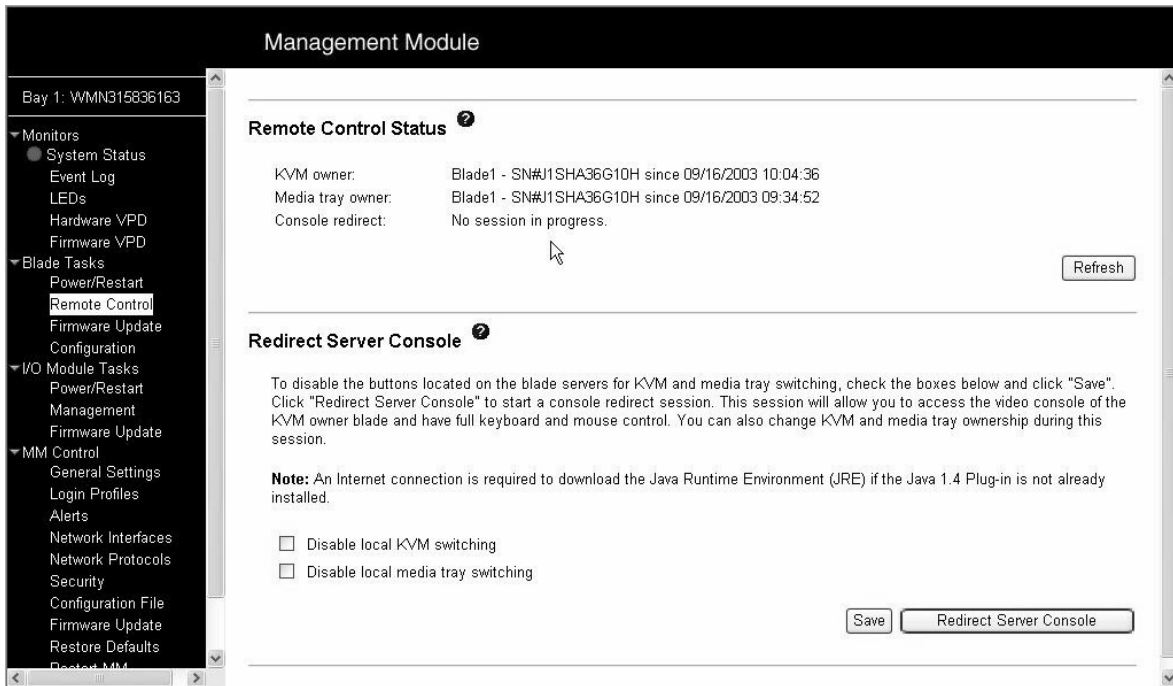
Remote control

Select this choice to:

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

  Notes:

1. Only one remote control session is allowed at a time. If a remote control session is already active, you can end the current session and start a new one.
2. The timeout value for a remote control session is the same as the timeout value that you set for the Web session when you logged in.
3. When you redirect a blade server Linux X Window System session console to the remote console, the ability of the remote console applet to accurately track the location of the mouse cursor depends on the configuration of X-Windows. Complete the following procedure to configure the X Window System for accurate mouse tracking. Type the commands through the remote console or at the keyboard attached to the SBCE unit. Note that the changes require root privileges.
   a. Enter the following commands:

      init 3 (Switch to text mode if necessary)

      rmmod mousedev (Unload the mouse driver module)

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

xset m 1 1 (Turn off mouse acceleration)

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

options mousedev xres=X yres=Y (Notify the mouse driver of the video resolution) where X and Y specify the video resolution

d. Enter the following commands:

insmod mousedev (Reload the mouse driver module)

init 5 (Return to GUI mode if necessary)

Firmware update
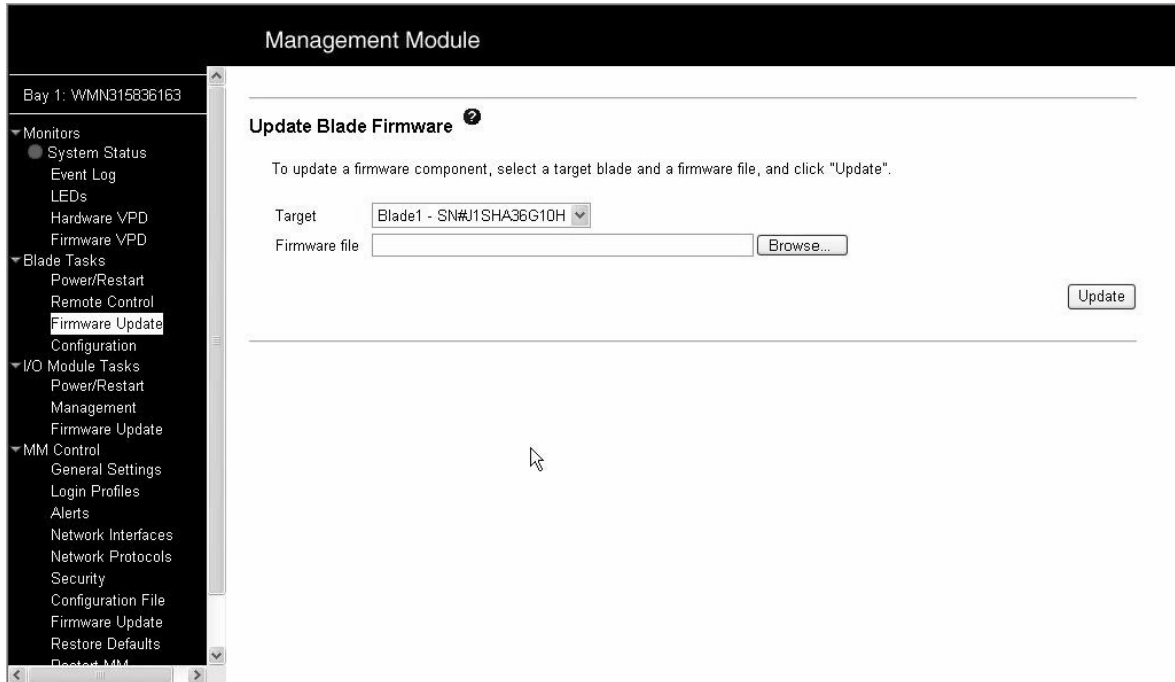
Select this choice to update the service processor firmware on a blade server. Select the target blade server and the firmware file to use for the update, then click **Update**.

Blade Service processor firmware update procedures

1. Open a Web browser. In the address or URL field, type the IP address or host name of the Management Module to which you want to connect. The Enter Network Password window opens.

✎ **NOTE**
The Management Module defaults to DHCP. If a DHCP host is unavailable, the Management Module assigns a static IP address of 192.168.70.125.

2. Type your user name and password in the Enter Network Password window. If you are using the Management Module for the first time, you can obtain your user name and password from your system administrator. All login attempts are documented in the event log. A welcome page opens in your browser.

✎ **NOTE**
The Management Module is set initially with a user name of USERID and password of PASSW0RD (with a zero, not an O). This user has read/write access. Change this default password during your initial configuration for enhanced security.

3. Select a timeout value, in minutes, in the field provided. If your browser is inactive for that number of minutes, the Management Module logs you off the Web interface.

4. Click Continue to start the session. The browser opens the System Health page, which gives you a quick view of the system status.

5. In the navigation frame under the Blade tasks heading, click Firmware Update, then click Browse.

6. Navigate to the PKT file you want to update.

7. Click Open. The file (including the full path) appears in the box beside Browse

8. To begin the update process, click Update. A progress indicator opens as the file is transferred to temporary storage on the Management Module. A confirmation page opens when the file transfer is completed.

9. Verify that the PKT file shown on the Confirm Firmware Update page is what you intend to update. If not, click the Cancel button.

10. To complete the update process, click Continue. A progress indicator opens as the firmware on the Blade Server Integrated System Management   Processor is flashed. A confirmation page opens to verify that the update was successful.

☞ **NOTE**

To cancel this process at any point, click Cancel.

Configuration
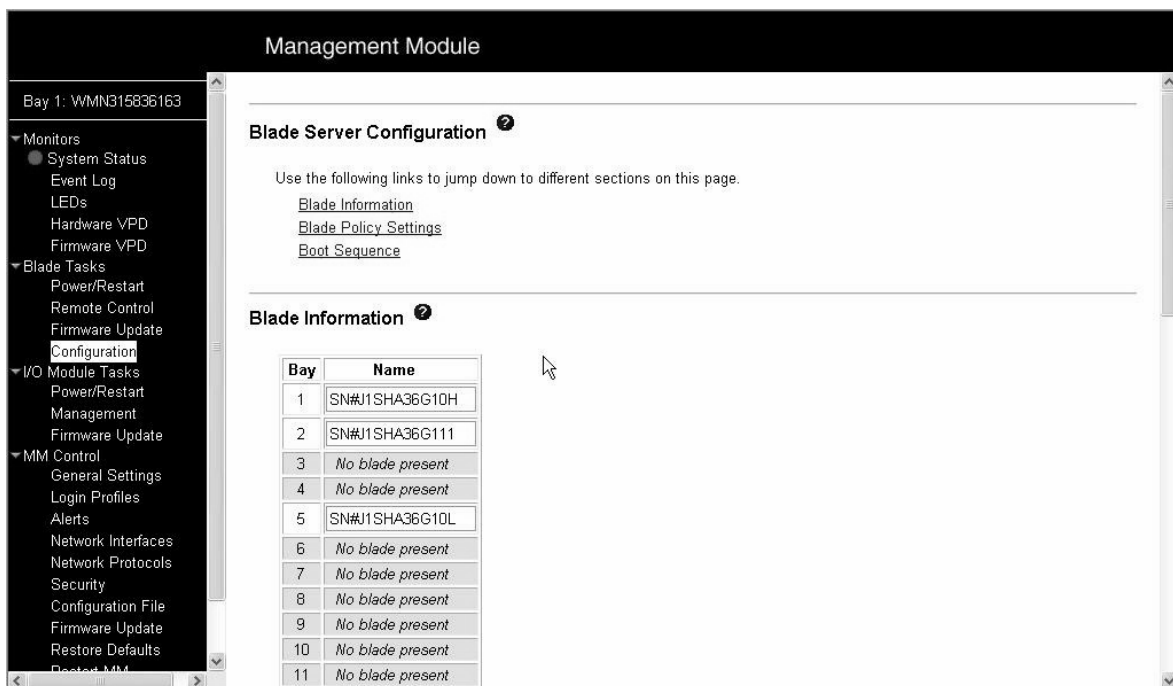
Select this choice to:

- Define a name for a blade server.
- Enable or disable the following items on all blade servers in the SBCE unit:
  — Local power control
  — Local KVM control
  — Local media tray control
  — The Wake on LAN feature

- View or define the startup (boot) sequence for one or more blade servers. The startup sequence prioritizes the following boot-record sources for a blade server:
  — IDE drive 1 (HDD1)
  — IDE drive 2 (HDD2)
  — CD-ROM
  — Diskette
  — Network
    – **PXE -** Attempt a PXE/DHCP network startup the next time the selected blade server is turned on or restarted.

✎ **NOTE**

In order to use the CD-ROM drive or diskette drive as a boot-record source for a blade server, the blade server must have been designated as the owner of the CD-ROM drive, diskette drive, and USB port. You set ownership either by pressing the CD/diskette/USB select button on the blade server or through the **Remote Control** choice described in "Configuring the management module for remote access" on page 19.

I/O Module Tasks

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

Power/Restart

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

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

Management
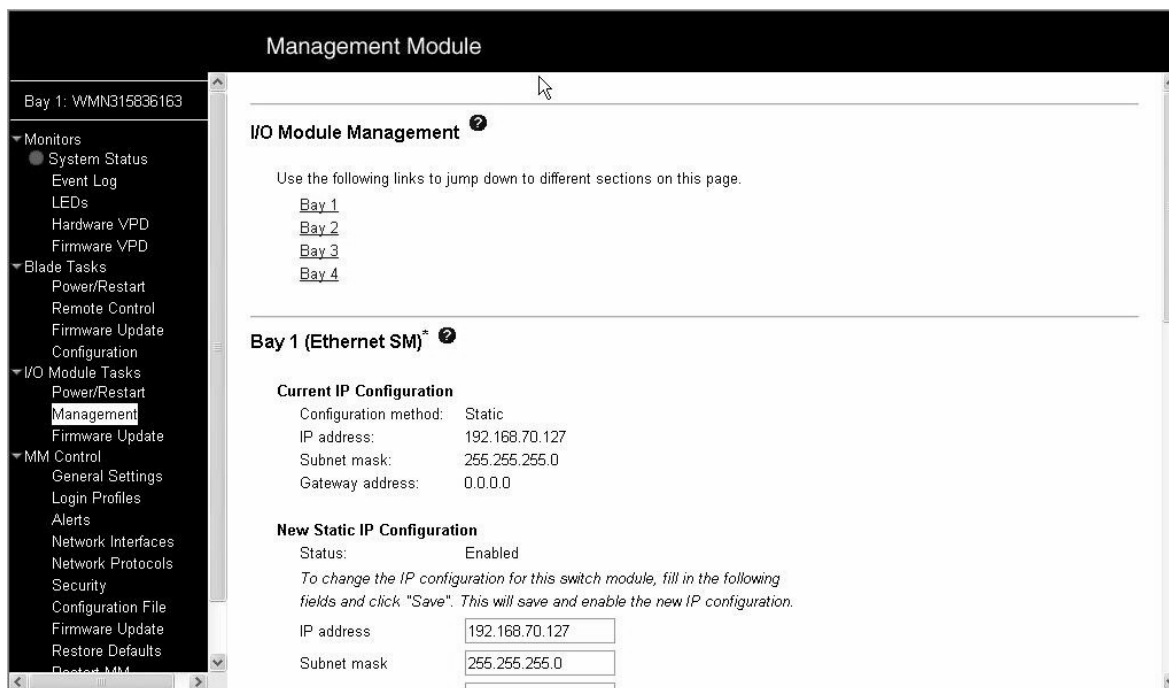
Select this choice to view or change the IP configuration of the Ethernet or Fibre Channel switch modules, ping the switch module, return a switch module to the default configuration, and start the configuration and management firmware that is in the switch module.

✏ **NOTE**
> Before you can access the switch module firmware, the following items must be set to **Enabled:**

- Switch module external ports
- External management for the external ports

From this page, click **Advanced Switch Management Advanced Setup** and enable the items.

The initial user ID and password for the switch module firmware are:

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

See the *Intel® Server Switch Module SBCEGBESW Installation and User's Guide* for more information about basic configuration of the 4 port Gb Ethernet switch module that is required for the SBCE unit.

See the documentation that comes with the switch module for details about the configuration and management firmware for the switch module. Documentation for the Ethernet switch module can be found on the SBCEGBESW Resource CD.

MM Control

Select the choices in this section to view and change the settings or configuration on the management module whose Web interface you are logged into. This includes configuring the following items:

- The name of the management module
- Up to 12 login profiles for logging in to the management module
- How alerts are handled

- The management module Ethernet connections for remote console and for communicating with the I/O modules
- Settings for the SNMP, SMTP, and DNS protocols
- Settings for secure socket layer (SSL) security

This also includes performing the following tasks:

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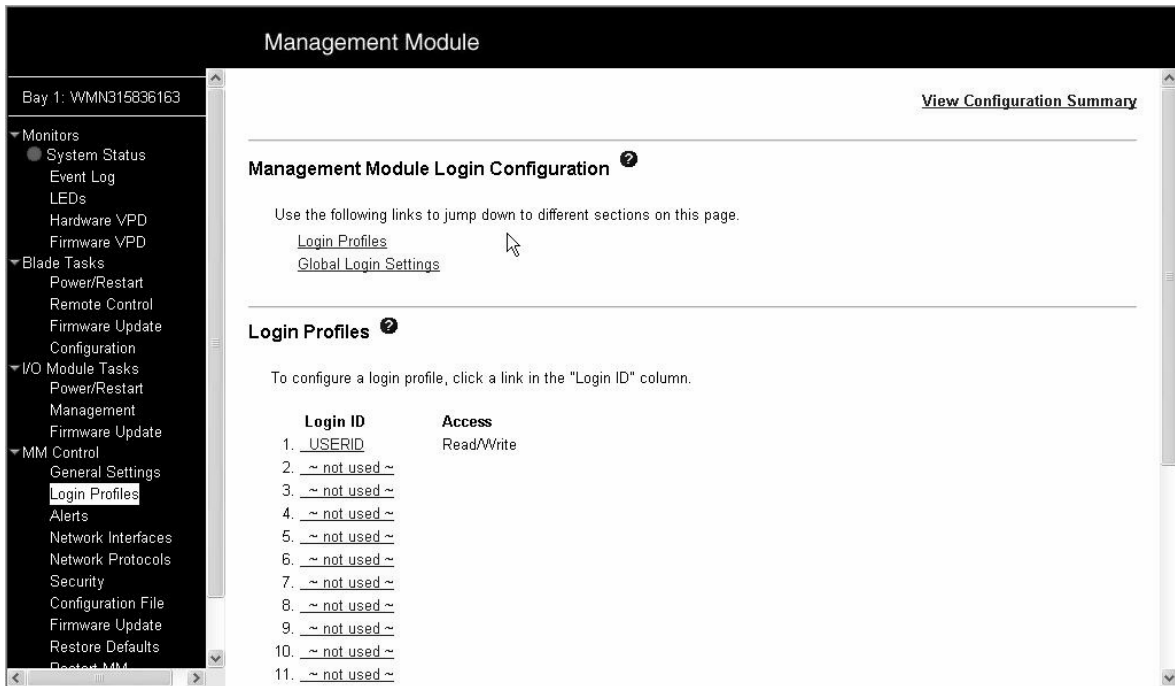- Switching from the current, active management module to the redundant management module

General Settings

Select this choice to view or change the following settings:

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

Login Profiles

Select this choice to configure up to 12 login profiles for logging in to the management module, and to specify the lockout period after five unsuccessful login attempts. For each profile, specify the following values:

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

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

Alerts

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

Network Interfaces

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

Notes:

1. When you use the management module Web interface to update the Ethernet or Fibre Channel switch module configuration, the management module firmware writes its settings for the switch module only to the management module NVRAM; it does not write its settings for the switch module to the switch module NVRAM.

   If the switch module restarts when the management module is not able to apply the IP address it has in NVRAM for the switch module, the switch module will use whatever IP address it has in its own NVRAM. If the two IP addresses are not the same, you might not be able to manage the Ethernet switch module any more.

   The management module cannot apply the switch IP address from its NVRAM if:

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

   You must use the Telnet interface to log into the switch module, change the IP address to match the one you assigned through the management module, and save the switch settings in the Telnet session (**Basic Setup>Save Changes**).

2. For switch communication with a remote management station, through the management module external Ethernet port, the switch module internal network interface and the management module internal and external interfaces must be on the same subnet.

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

     ✏ **NOTE**

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

   — **Interface -** Select Enabled (the default) to use the Ethernet connection.

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

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

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

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

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

       • **IP address** - The IP address for the management module. The IP address must contain four integers from 0 to 255, separated by periods, with no spaces or consecutive periods. The default setting is 192.168.70.125.

       • **Subnet mask** - The subnet mask must contain four integers from 0 to 255, separated by periods, with no spaces. The default setting is 255.255.255.0

       • **Gateway address** - The IP address for your network gateway router. The gateway address must contain four integers from 0 to 255, separated by periods, with no spaces.

- **Internal Network Interface (eth1)** - This interface communicates with the network-interface I/O modules, such as the Ethernet switch module or the Fibre Channel switch module.

   — Specify the IP address to use for this interface. The subnet mask must be the same as the subnet mask in the external network interface (eth0).

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

   — You can configure the internal Ethernet management port on each switch module in the SBCE unit. First click on **MM Control>Network interfaces**. Click Switch Module 1. From this page, click **Advanced Switch Management>Advanced Setup** and enable the following items:

     - Switch module external ports
     - External management for the external ports

✏ **NOTE**
      The initial ID and Password for the switch module firmware are:

- **User ID: USERID (all capital letters)**

Password: PASSW0RD (note the zero, not O, in PASSW0RD)

   — Specify the IP configuration of the switch module

   — Repeat this step for each switch module in the SBCE unit

To communicate with the blade servers for functions such as deploying an operating system or application program, you also will need to configure at least one external (in-band) port on an Ethernet switch module. See the Intel® Server Chassis SBCE Installation and User's Guide for information about configuring external ports on Ethernet switch modules.

- **TCP log** - Select this choice to view entries that are currently stored in the management module TCP log. This log contains error and warning messages generated by the TCP/IP code running on the management module, and might be used by your service representative for advanced troubleshooting. The log displays the most recent entries first.

You can sort and filter entries in the event log.

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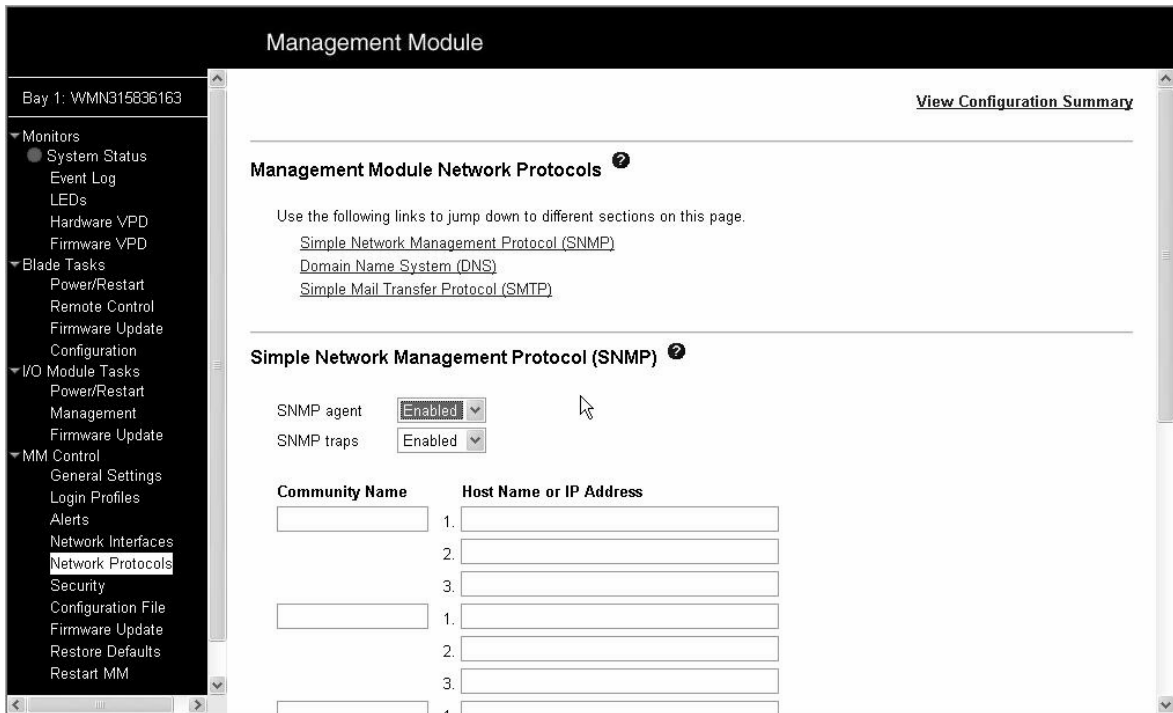
Select this choice to view or change the settings for the SNMP, SMTP, and DNS protocols.

Security

Select this choice to view or change the secure socket layer (SSL) settings. You can enable or disable (the default) SSL, and choose between self-signed certificates and certificates provided by a certificate authority (CA).

> ✏ **NOTE**
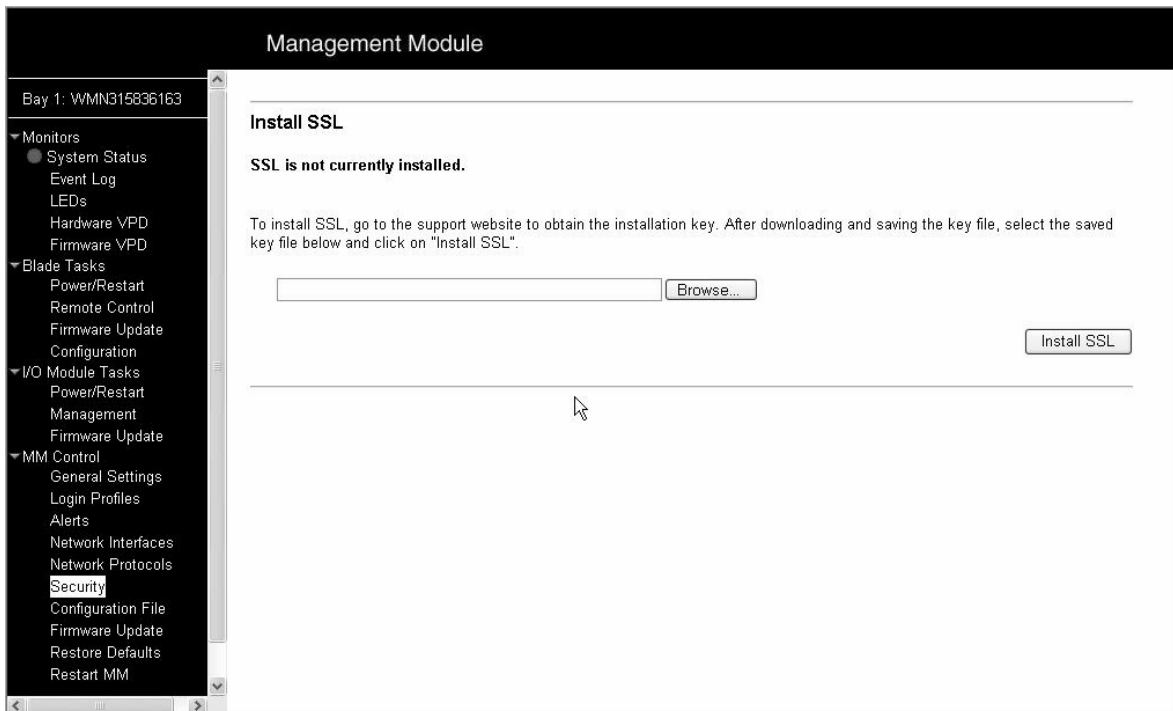>> The first time you select Security, you are directed to a Web page for downloading the SSL installation key as follows:

1. Go to http://downloadfinder.intel.com, type "SSL" in the Download Search box and click Go!

2. Scan the search results list and click on "Intel® Server Chassis SBCE".

3. Under "select your operating system", select "OS Independent" from the drop-down menu and Click Go!

4. Click on the "Intel® Server Management Module SBCECMM SSL Installation Key [SSL_INSTALL.EXE]" and follow the online instructions to download the SSL key.

5. You should receive a response from the Encryption Coordinator within 2 business days, containing a link to the file and a password. Using this information, download and save the file.

6. After saving the SSL key file, browse to the SSL key file in the MM Security screen and click on "Install SSL".

7. After you load the key, the Security choice functions as described.

Configuration File
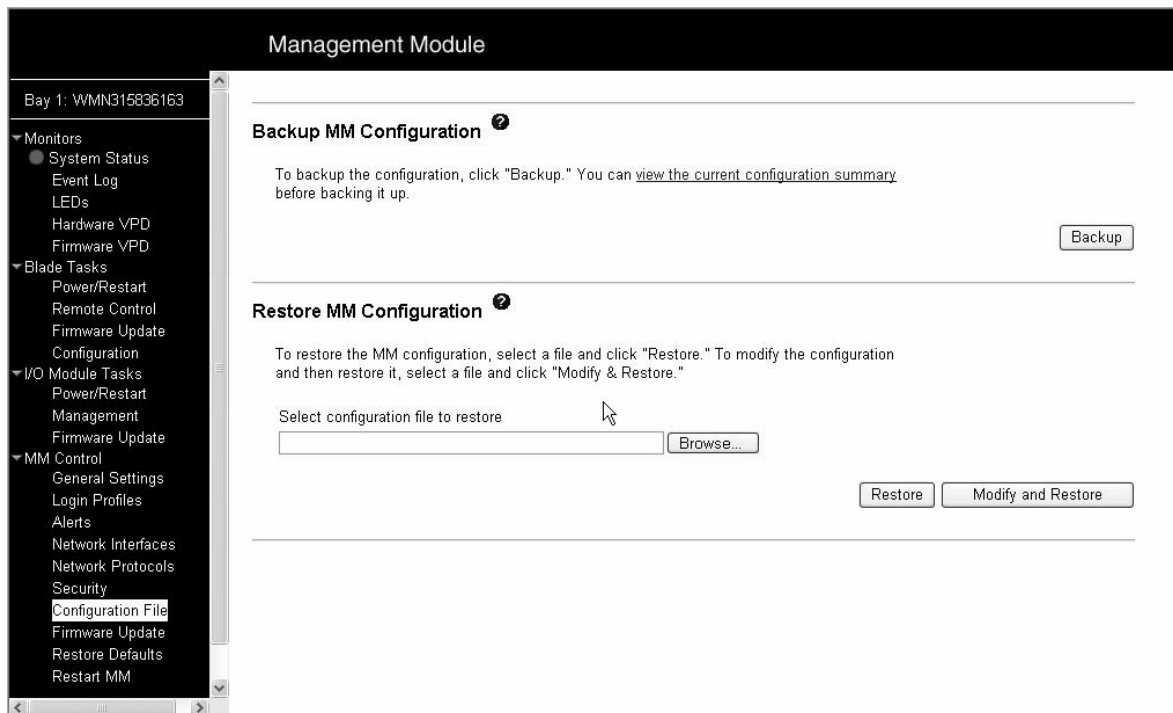
Select this choice to back up or restore the management module configuration file.

Firmware Update
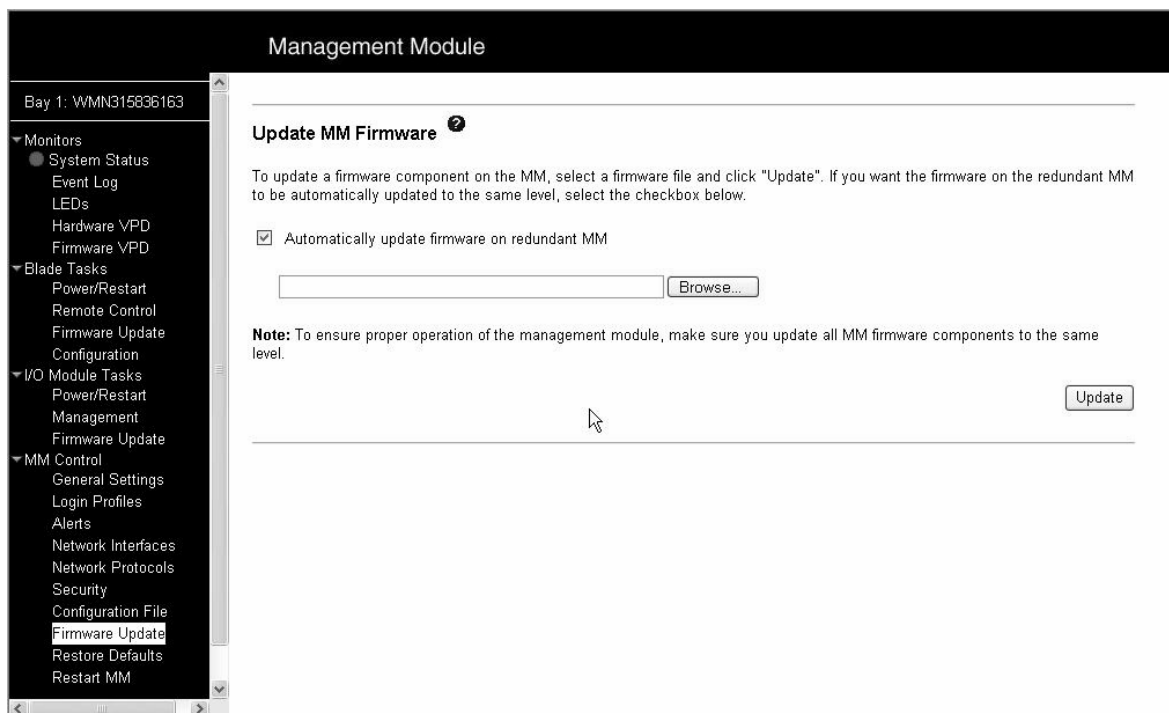
Select this choice to update the management module firmware.

If a second management module is installed, you can choose to apply the firmware update only to the active management module. Follow the procedures below to update the management module firmware.

Chassis management module firmware update procedures

This section provides instructions for updating the firmware on your Intel® Server Management Module SBCECMM.

1. Copy the latest management module update files to a floppy diskette.   The management module firmware files will be updated through the CMM web interface via a console client. The firmware files should include the following components.

    • CNETBRUS.PKT
    • CNETMNUS.PKT
    • CNETRGUS.PKT
    • *REMOTEKM.PKT
    • *DUALPS2.PKT

2. Open a Web browser. In the address or URL field, type the IP address or host name of the Management Module to which you want to connect. The Enter Network Password window opens.

    ✏ **NOTE**
    The Management Module defaults to DHCP. If a DHCP host is unavailable, the Management Module assigns a static IP address of 192.168.70.125.

3. Type your user name and password in the Enter Network Password window. If you are using the Management Module for the first time, you can obtain your user name and password from your system administrator. All login attempts are documented in the event log. A welcome page opens in your browser.

✏ **NOTE**
> The Management Module is set initially with a user name of USERID and password of PASSW0RD (with a zero, not an O). This user has read/write access. Change this default password during your initial configuration for enhanced security.

4. Select a timeout value, in minutes, in the field provided. If your browser is inactive for that number of minutes, the Management Module logs you off the Web interface.

5. Click Continue to start the session. The browser opens the System Health page, which gives you a quick view of the system status.

6. In the navigation frame, click MM Firmware Update under MM Control, then click Browse.

7. Navigate to the PKT file you want to update.

✏ **NOTE**
> There are five packet files that should be updated:

- CNETBRUS.PKT
- CNETMNUS.PKT
- CNETRGUS.PKT
- **REMOTEKM.PKT
- **DUALPS2.PKT

✏ **NOTE**
> **Does not require a Management Module restart

8. Click Open. The file (including the full path) appears in the box beside Browse.

9. To begin the update process, click Update. A progress indicator opens as the file is transferred to temporary storage on the Management Module. A confirmation page opens when the file transfer is completed.

10. Verify that the PKT file shown on the Confirm Firmware Update page is what you intend to update. If not, click the Cancel button.

11. To complete the update process, click Continue. A progress indicator opens as the firmware on the Management Module is flashed. A confirmation page opens to verify that the update was successful.

12. Repeat steps 6 through 11 for each packet on this diskette.

13. After receiving a confirmation that the update process is complete, click the option "Restart MM" and click the Restart button. Click OK to confirm that you want to restart the Management Module.

✏ **NOTE**
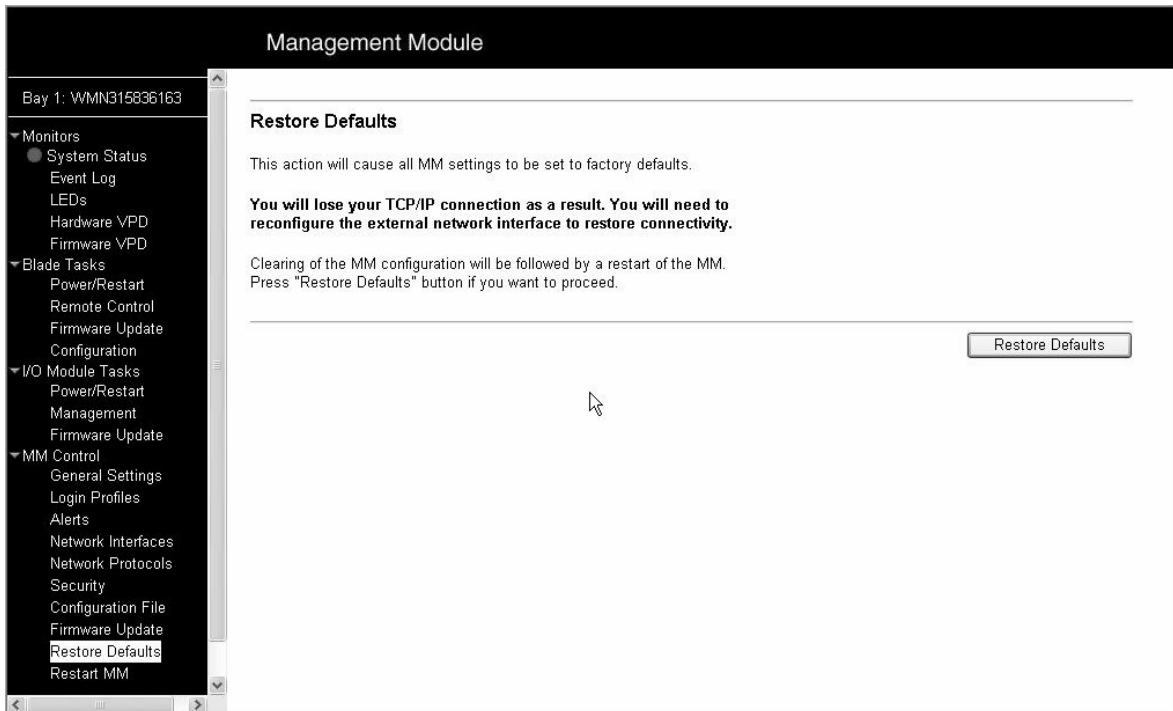> Restarting the Management Module will disconnect your current session.

14. Click OK to close the current browser window.

15. To log into the Management Module again, open your browser and follow the regular login process.
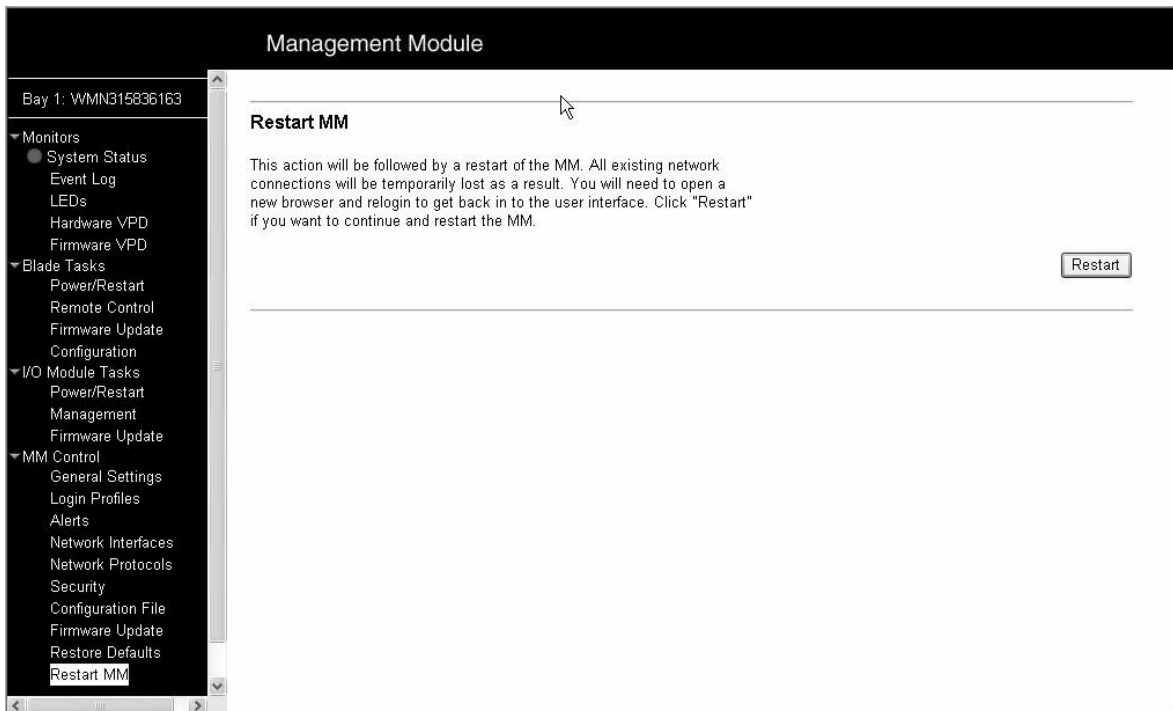
✏ **NOTE**
> To cancel this process at any point, click Cancel.

Restore Defaults

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

Restart MM

Select this choice to restart (reset) the management module or to change to the redundant management module if one is present.

Configuring SNMP

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

> ✏ **NOTE**
> If you plan to configure Simple Network Management Protocol (SNMP) traps on the management module, you must install and compile the management information base (MIB) on your SNMP manager, The MIB supports SNMP traps. The MIB is included in the management module firmware update package that you downloaded from the Intel Support Web Site.

Complete the following steps to configure your SNMP:

1. Log in to the management module where you want to configure SNMP.
2. In the navigation pane, click General Settings. In the management module information page that opens, specify the following information:
   - Management module name - The name that you want to use to identify the management module. The name will be included with e-mail and SNMP alert notifications to identify the source of the alert.
   - System contact - The name and phone number of the person to contact if there is a problem with the SBCE unit.
   - System location - Sufficient detail to quickly locate the SBCE unit for maintenance or other purposes.
3. Scroll to the bottom of the page and click Save.
4. In the navigation pane, click Network Protocols; then, click the Simple Network Management Protocol (SNMP) link.
5. Select Enabled in the SNMP agent and SNMP traps fields to forward alerts to SNMP communities on your network. To enable the SNMP agent, the following criteria must be met:
   - System contacts must be specified on the General Settings page.
   - The system location must be specified on the General Settings page.
   - At least one community name must be specified.
   - At least one valid IP address or host name (if DNS is enabled) must be specified for that community.

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

6. Set up a community to define the administrative relationship between SNMP agents and SNMP managers. You must define at least one community. Each community definition consists of the following parameters:
   - Name
   - IP address

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

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

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

11. If DNS server (or servers) is available on your network, select Enabled in the DNS field. The DNS field specifies whether you use a DNS server on your network to translate host names into IP addresses.

12. If you enabled DNS, in the DNS server IP address fields, you can specify the IP addresses of up to three DNS servers on your network, Each IP address should contain integers from 0 through 255, separated by periods.

13. Scroll to the bottom of the page and click Save. In the navigation pane, click Restart MM to activate the changes.

Saving the configuration file

After you have configured the management module, you can save the configuration file to a diskette or other external media. Then, if the configuration in the management module becomes damaged or the management module is replaced, you can restore the saved configuration file to the management module. Use the management module Web interface to save and restore the configuration file (**MM Control Configuration File**).

The IP address may also be obtained by running the Intel® Blades Discovery Console (IBDC). The IBDC software will discover all active management modules that are on the same subnet as the client console.

Restoring a saved configuration file

If you have a saved configuration file, you can apply it to the primary or only management module.

1. After the primary or only management module has been installed, follow the instructions in "Setting up the remote connection" on page 46 through "Configuring the management module for remote access" on page 47.

2. Follow the instructions in "Starting the management and configuration program" on page 48.

3. In the MM Control section in the navigation pane, click **Configuration File** and follow the instructions under **Restore MM Configuration** to apply the saved configuration file.

✏ **NOTE**

If a second management module is installed in the SBCE unit (see "Preparing for management module redundancy" on page 8 for more information), the new configuration information will be transferred to the secondary management module automatically.If you cannot communicate with a replacement management module through the Web interface, the IP address might be different from the IP address of the management module just removed. Press the IP reset button to set the management module to the factory default IP addresses. Then, access the management module using the factory IP address. See, "Configuring the management module for remote access," on page 19, for the factory IP addresses, and configure the management module or load the saved configuration file.

A Getting help and technical assistance

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 SBCE unit 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 SBCE unit 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.

\<This page intentionally left blank\>

Index

A

acoustic attenuation module 11

B

bay locations 7

C

cabling
    keyboard, video, and mouse 15
    remote connection Ethernet port 18
components
    major 3
configuration file
    restoring 44
    saving 44
Configuration/Setup Utility program 20
connector
    Ethernet
        remote management and console 6
    input/output 5
    keyboard 5
    PS/2 mouse 6
    remote management 6
    video 5

D

difficulty communicating with replacement module 44

E

error log. See event log
Ethernet
    configuring remote connection 19
    port, cabling 18
Ethernet activity LED 4, 18
Ethernet connector, remote management and console 6
Ethernet-link status LED 4, 18
event log 24
event log in alerts 35
event log, viewing 24

H

handling static-sensitive devices 8

I

identification labels 3
installation
    guidelines 7

S

saving configuration file 44
serial number 3
static electricity 8
static-sensitive devices, handling 8
system reliability 7

T

TCP log 37
TCP log, viewing 37

U

utility, Configuration/Setup 20

V

video connector 5

W

Web site
    compatible options 7