Lenovo Flex System Enterprise Chassis Installation and Service Guide

Machine Type: 7893, 8721, 8724

Note

Before using this information and the product it supports, read the general information in Appendix B “Notices” on page 1007; and read the *Safety Information* and the *Environmental Notices and User Guide* on the Lenovo *Documentation CD*.

Eleventh Edition (May 2022)

Contents

Safety

Before installing this product, read the Safety Information.

قبل تركيب هذا المنتج، يجب قراءة الملاحظات الآمنية

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

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

安裝本產品之前，請先閱讀「安全資訊」。

Prije instalacije ovog produkta obavezno pročitajte Sigurnosne Upute.

Před instalací tohoto produktu si přečtěte příručku bezpečnostních instrukcí.

Læs sikkerhedsforskrifterne, før du installerer dette produkt.

Lees voordat u dit product installeert eerst de veiligheidsvoorschriften.

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

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

Vor der Installation dieses Produkts die Sicherheitshinweise lesen.

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

לפני שתתקינו מוצר זה, קראו את הוראות הבטיחות.

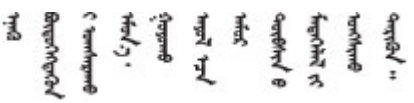
A termék telepítése előtt olvassa el a Biztonsági előírásokat!

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

製品の設置の前に、安全情報をお読みください。

본 제품을 설치하기 전에 안전 정보를 읽으십시오.

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



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

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

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

Перед установкой продукта прочтите инструкции по
технике безопасности.

Pred inštaláciou tohto zariadenia si pečítaje Bezpečnostné predpisy.

Pred namestitvijo tega proizvoda preberite Varnostne informacije.

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

Läs säkerhetsinformationen innan du installerar den här produkten.

ཐོན་རྫས་འདི་བདེ་སྤྱོད་མ་བྱས་གོང་། ·སྐོར་གྱི་ཡིད་གཟབ·
བྱ་འདྲ་མིན་ཡོད་པའི་འོད་སྣེར་བལྟ་དགོས།

Bu ürünü kurmadan önce güvenlik bilgilerini okuyun.

مەزكۇر مەھسۇلاتنى ئورنىتىشتىن بۇرۇن بىخەتەرلىك ئۇچۇرلىرىنى ئوقۇپ چىقىڭ.

Youq mwngz yungh canjbinj neix gaxgonq, itdingh aeu doeg aen
canjbinj soengq cungj vahgangj ancien siusik.

Guidelines for trained service technicians

This section contains information for trained service technicians.

Inspecting for unsafe conditions

Use this information to help you identify potential unsafe conditions in a device that you are working on.

Each device, as it was designed and manufactured, has required safety items to protect users and service technicians from injury. The information in this section addresses only those items. Use good judgment to identify potential unsafe conditions that might be caused by unsupported alterations or attachment of unsupported features or optional devices that are not addressed in this section. If you identify an unsafe condition, you must determine how serious the hazard is and whether you must correct the problem before you work on the product.

Consider the following conditions and the safety hazards that they present:

- Electrical hazards, especially primary power. Primary voltage on the frame can cause serious or fatal electrical shock.
- Explosive hazards, such as a damaged CRT face or a bulging capacitor.
- Mechanical hazards, such as loose or missing hardware.

To inspect the product for potential unsafe conditions, complete the following steps:

1. Make sure that the power is off and the power cords are disconnected.
2. Make sure that the exterior cover is not damaged, loose, or broken, and observe any sharp edges.
3. Check the power cords:
   - Make sure that the third-wire ground connector is in good condition. Use a meter to measure third-wire ground continuity for 0.1 ohm or less between the external ground pin and the frame ground.
   - Make sure that the power cords are the correct type.

- Make sure that the insulation is not frayed or worn.

4. Remove the cover.
5. Check for any obvious unsupported alterations. Use good judgment as to the safety of any unsupported alterations.
6. Check inside the system for any obvious unsafe conditions, such as metal filings, contamination, water or other liquid, or signs of fire or smoke damage.
7. Check for worn, frayed, or pinched cables.
8. Make sure that the power-supply cover fasteners (screws or rivets) have not been removed or tampered with.

Guidelines for servicing electrical equipment

Observe these guidelines when you service electrical equipment.

- Check the area for electrical hazards such as moist floors, nongrounded power extension cords, and missing safety grounds.
- Use only approved tools and test equipment. Some hand tools have handles that are covered with a soft material that does not provide insulation from live electrical current.
- Regularly inspect and maintain your electrical hand tools for safe operational condition. Do not use worn or broken tools or testers.
- Do not touch the reflective surface of a dental mirror to a live electrical circuit. The surface is conductive and can cause personal injury or equipment damage if it touches a live electrical circuit.
- Some rubber floor mats contain small conductive fibers to decrease electrostatic discharge. Do not use this type of mat to protect yourself from electrical shock.
- Do not work alone under hazardous conditions or near equipment that has hazardous voltages.
- Locate the emergency power-off (EPO) switch, disconnecting switch, or electrical outlet so that you can turn off the power quickly in the event of an electrical accident.
- Disconnect all power before you perform a mechanical inspection, work near power supplies, or remove or install main units.
- Before you work on the equipment, disconnect the power cord. If you cannot disconnect the power cord, have the customer power-off the wall box that supplies power to the equipment and lock the wall box in the off position.
- Never assume that power has been disconnected from a circuit. Check it to make sure that it has been disconnected.
- If you have to work on equipment that has exposed electrical circuits, observe the following precautions:
  - Make sure that another person who is familiar with the power-off controls is near you and is available to turn off the power if necessary.
  - When you work with powered-on electrical equipment, use only one hand. Keep the other hand in your pocket or behind your back to avoid creating a complete circuit that could cause an electrical shock.
  - When you use a tester, set the controls correctly and use the approved probe leads and accessories for that tester.
  - Stand on a suitable rubber mat to insulate you from grounds such as metal floor strips and equipment frames.
- Use extreme care when you measure high voltages.
- To ensure proper grounding of components such as power supplies, pumps, blowers, fans, and motor generators, do not service these components outside of their normal operating locations.

- If an electrical accident occurs, use caution, turn off the power, and send another person to get medical aid.

Safety statements

These statements provide the caution and danger information that is used in this documentation.

Important: Each caution and danger statement in this documentation is labeled with a number. This number is used to cross reference an English-language caution or danger statement with translated versions of the caution or danger statement in the *Safety Information* document.

For example, if a caution statement is labeled `Statement 1`, translations for that caution statement are in the *Safety Information* document under `Statement 1`.

Be sure to read all caution and danger statements in this documentation before you perform the procedures. Read any additional safety information that comes with your system or optional device before you install the device.

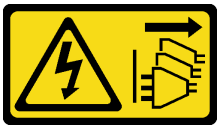
S001

DANGER

Electrical current from power, telephone, and communication cables is hazardous.
To avoid a shock hazard:

- **Connect all power cords to a properly wired and grounded electrical outlet/source.**
- **Connect any equipment that will be attached to this product to properly wired outlets/sources.**
- **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.**
- **The device might have more than one power cord, to remove all electrical current from the device, ensure that all power cords are disconnected from the power source.**

S002



CAUTION:
The power-control button on the device and the power switch on the power supply do not turn off the electrical current supplied to the device. The device also might have more than one power cord. To remove all electrical current from the device, ensure that all power cords are disconnected from the power source.

S003

CAUTION:
If you install a strain-relief bracket option over the end of the power cord that is connected to the device, you must connect the other end of the power cord to an easily accessible power source.

S004

CAUTION:
When replacing the lithium battery, use only Lenovo specified part number or an equivalent type battery recommended by the manufacturer. 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.

S005

CAUTION:
The battery is a lithium ion battery. To avoid possible explosion, do not burn the battery. Exchange it only with the approved part. Recycle or discard the battery as instructed by local regulations.

S006

CAUTION:
When laser products (such as CD-ROMs, DVD 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.**

S007

CAUTION:
This product contains a Class 1M laser. Do not view directly with optical instruments.

S008

DANGER

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

S009

CAUTION:
To avoid personal injury, disconnect the fan cables before removing the fan from the device.

S010

CAUTION:
Do not place any object weighing more than 82 kg (180 lb) on top of rack-mounted devices.

S011

CAUTION:
Sharp edges, corners, or joints nearby.

S012

CAUTION:
Hot surface nearby.

S013

DANGER

Overloading a branch circuit is potentially a fire hazard and a shock hazard under certain conditions. To avoid these hazards, ensure that your system electrical requirements do not exceed branch circuit protection requirements. Refer to the information that is provided with your device for electrical specifications.

S014

CAUTION:
Hazardous voltage, current, and energy levels might be present. Only a qualified service technician is authorized to remove the covers where the label is attached.

S015

CAUTION:
Make sure that the rack is secured properly to avoid tipping when the server unit is extended.

S016

CAUTION:
Some accessory or option board outputs exceed Class 2 or limited power source limits and must be installed with appropriate interconnecting cabling in accordance with the national electric code.

S017

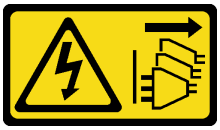
CAUTION:
Hazardous moving fan blades nearby. Keep fingers and other body parts away.

S018

CAUTION:
To reduce the risk of electric shock or energy hazards:

- **This equipment must be installed or serviced by trained personnel in a restricted-access location, as defined by the NEC, IEC 62368-1 and IEC 60950-1, the standard for Safety of Electronic Equipment within the Field of Audio/Video, Information Technology and Communication Technology.**
- **Connect the equipment to a reliably grounded safety extra low voltage (SELV) source. An SELV source is a secondary circuit that is designed so that normal and single fault conditions do not cause the voltages to exceed a safe level (60 V direct current).**
- **The branch circuit overcurrent protection must be rated at a minimum of 5 A to a maximum of 15 A.**
- **Use 14 American Wire Gauge (AWG) or 2.5 mm^2 copper conductor only, not exceeding 3 meters in length.**
- **Torque the wiring-terminal screws to 12 inch-pounds (1.4 newton-meters).**
- **Incorporate a readily available approved and rated disconnect device in the field wiring.**

S019



CAUTION:
The power-control button on the device does not turn off the electrical current supplied to the device. The device also might have more than one connection to dc power. To remove all electrical current from the device, ensure that all connections to dc power are disconnected at the dc power input terminals.

S020

CAUTION:
To avoid personal injury, before lifting the unit, remove all the blades to reduce the weight.

S021

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

S022

CAUTION:
To reduce the risk of electric shock or energy hazards:

- **This equipment must be installed or serviced by trained personnel in a restricted-access location, as defined by the NEC, IEC 62368-1 and IEC 60950-1, the standard for Safety of Electronic Equipment within the Field of Audio/Video, Information Technology and Communication Technology.**
- **Connect the equipment to a reliably grounded safety extra low voltage (SELV) source. An SELV source is a secondary circuit that is designed so that normal and single fault conditions do not cause the voltages to exceed a safe level (60 V direct current).**
- **The branch circuit overcurrent protection must be rated at a minimum of 13 A to a maximum of 15 A.**
- **Use 16 American Wire Gauge (AWG) or 1.3 mm^2 copper conductor only, not exceeding 3 meters in length.**
- **Torque the wiring-terminal screws to 12 inch-pounds (1.4 newton-meters).**
- **Incorporate a readily available approved and rated disconnect device in the field wiring.**

S023

CAUTION:
Do not place any object weighing more than 50 kg (110 lb) on top of rack-mounted devices.

S024

CAUTION:
To reduce the risk of electric shock or energy hazards:

- **This equipment must be installed or serviced by trained personnel in a restricted-access location, as defined by the NEC, IEC 62368-1 and IEC 60950-1, the standard for Safety of Electronic Equipment within the Field of Audio/Video, Information Technology and Communication Technology.**
- **Connect the equipment to a reliably grounded safety extra low voltage (SELV) source. An SELV source is a secondary circuit that is designed so that normal and single fault conditions do not cause the voltages to exceed a safe level (60 V direct current).**
- **The branch circuit overcurrent protection must be rated at a minimum of 12 A to a maximum of 15 A.**
- **Use 14 American Wire Gauge (AWG) or 2.5 mm^2 copper conductor only, not exceeding 3 meters in length.**
- **Torque the wiring-terminal screws to 12 inch-pounds (1.4 newton-meters).**
- **Incorporate a readily available approved and rated disconnect device in the field wiring.**

S025

CAUTION:
Do not place any object on top of rack-mounted devices.

S026

CAUTION:
Hazardous moving parts are nearby.

S027

CAUTION:
This equipment is designed to permit the connection of the earthed conductor of the dc supply circuit to the earthing conductor at the equipment. If this connection is made, all of the following conditions must be met:

- **This equipment shall be connected directly to the dc supply system earthing electrode conductor or to a bonding jumper from an earthing terminal bar or bus to which the dc supply system earthing electrode conductor is connected.**
- **This equipment shall be located in the same immediate area (such as, adjacent cabinets) as any other equipment that has a connection between the earthed conductor of the same dc supply circuit and the earthing conductor, and also the point of earthing of the dc system. The dc system shall not be earthed elsewhere.**
- **The dc supply source shall be located within the same premises as this equipment.**

- **Switching or disconnecting devices shall not be in the earthed circuit conductor between the dc source and the point of connection of the earthing electrode conductor.**

S028

CAUTION:
To reduce the risk of electric shock or energy hazards:

- **This equipment must be installed or serviced by trained personnel in a restricted-access location, as defined by the NEC, IEC 62368-1 and IEC 60950-1, the standard for Safety of Electronic Equipment within the Field of Audio/Video, Information Technology and Communication Technology.**
- **Connect the equipment to a reliably grounded safety extra low voltage (SELV) source. An SELV source is a secondary circuit that is designed so that normal and single fault conditions do not cause the voltages to exceed a safe level (60 V direct current).**
- **The branch circuit overcurrent protection must be rated 20 A.**
- **Use 12 American Wire Gauge (AWG) or 2.5 mm^2 copper conductor only, not exceeding 4.5 meters in length.**
- **Incorporate a readily available approved and rated disconnect device in the field wiring.**

S029

DANGER

For -48V dc power supply, electrical current from power cables is hazardous.
To avoid a shock hazard:

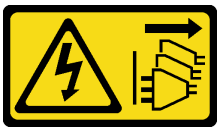
- **To connect or disconnect -48V dc power cables when you need to remove/replace install redundancy power supply unit(s).**

To Connect:	To Disconnect:
1. Turn OFF subject dc power source(s) and equipment (s) that are attached to this product. 2. Install the power supply unit(s) into the system housing. 3. Attach dc power cable(s) to the product. • Ensure correct polarity of -48 V dc connections: RTN is + and -48 V dc is -. Earth ground should use a two-hole lug for safety. 4. Connect dc power cable(s) to subject power source (s). 5. Turn ON all the power source(s).	1. Disconnect or turn off the subject dc power source(s) (at the breaker panel) before removing the power supply unit(s). 2. Remove the subject dc cable(s). 3. Unplug the subject power supply unit(s) from the system housing.

S030

CAUTION:
To avoid personal injury, before lifting the unit, remove all the blades, power modules, and other removable modules to reduce the weight.

S031



CAUTION:
This product does not provide a power-control button. Turning off blades or removing power modules and I/O modules does not turn off electrical current supplied to the product. The product also might have more than one power cord. To remove all electrical current from the product, ensure that all power cords are disconnected from the power source.

S032

CAUTION:
To reduce the risk of electric shock or energy hazards:

- **This equipment must be installed or serviced by trained personnel in a restricted-access location, as defined by the NEC, IEC 62368-1 and IEC 60950-1, the standard for Safety of Electronic Equipment within the Field of Audio/Video, Information Technology and Communication Technology.**

- **Connect the equipment to a properly grounded safety extra low voltage (SELV) source. A SELV source is a secondary circuit that is designed so that normal and single fault conditions do not cause the voltages to exceed a safe level (60 V direct current).**
- **See the specifications in the product documentation for the required circuit-breaker rating for branch circuit overcurrent protection.**
- **Use copper wire conductors only. See the specifications in the product documentation for the required wire size.**
- **See the specifications in the product documentation for the required torque values for the wiring-terminal screws.**
- **Incorporate a readily available approved and rated disconnect device in the field wiring.**

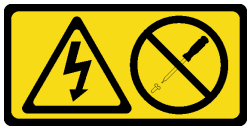
S033

CAUTION:
Hazardous energy present. Voltages with hazardous energy might cause heating when shorted with metal, which might result in spattered metal, burns, or both.

S034

CAUTION:
Always install the slide retention screw.

S035



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

S036

18 - 32 kg (39 - 70 lb)

32 - 55 kg (70 - 121 lb)

CAUTION:
Use safe practices when lifting.

S037

CAUTION:
The weight of this part or unit is more than 55 kg (121.2 lb). It takes specially trained persons, a lifting device, or both to safely lift this part or unit.

R002

DANGER

- **Always lower the leveling pads on the rack cabinet.**
- **Always install stabilizer brackets on the rack cabinet.**
- **Always install the heaviest devices in the bottom of the rack cabinet.**
- **Always install servers and optional devices starting from the bottom of the rack cabinet.**

UL regulatory information

This device is for use only with Listed chassis.

Attention: This product is suitable for use on an IT power distribution system whose maximum phase-to phase-voltage is 240 V under any distribution fault condition.

Chapter 1. Introduction

The Lenovo Flex System Enterprise Chassis Types 7893, 8721, and 8724 is a 10U next-generation server platform with integrated chassis management. It is a compact, high-density, high-performance, rack-mounted, scalable server platform system.

The Flex System Enterprise Chassis has fourteen node bays that support up to fourteen 1-bay compute nodes or up to seven 2-bay compute nodes when the shelves are removed from the chassis. You can use both 1-bay and 2-bay compute nodes to meet your specific hardware needs.

The Flex System Enterprise Chassis also supports 4-bay storage nodes, when the shelves and shelf supports are removed from the chassis. The Flex System Enterprise Chassis can support up to three 4-bay storage nodes or storage expansion enclosures.

The compute nodesand storage nodes share common resources, such as power, cooling, management, and I/O resources in the chassis.

Note:

- A 1-bay compute node occupies one node bay in the chassis.
- A 1-bay compute node with captive-mode expansion node occupies two adjacent node bays (horizontally) in the chassis and requires the chassis shelf to be removed prior to installation.
- A 2-bay compute node occupies two adjacent node bays (horizontally) in the chassis and requires the chassis shelf to be removed prior to installation.
- A 4-bay storage node or storage expansion enclosure occupies four adjacent node bays (two vertically and horizontally) in the chassis and requires the chassis shelves and shelf supports to be removed prior to installation.

The Flex System Enterprise Chassis can support the following components:

- Up to fourteen 1-bay compute nodes or up to seven 2-bay compute nodes with the shelves removed.
- Up to seven 1-bay compute nodes with captive-mode expansion node (each assembly occupies two node bays).
- Up three 4-bay storage nodes or storage expansion enclosures with the shelves and shelf supports removed.
- Up to six power supplies. 200-240 V ac power supplies, 240-380 V dc power supplies, and -48 V to -60 V dc power supplies are available.
- Up to ten fan modules (two 40 mm fan modules and eight 80 mm fan modules).
- Four I/O modules (two redundant pairs), with the following features in each module:
  - A four-lane physical interconnect that supports speeds up to 16 Gbps, four-lanes to each single node bay or eight-lanes to each full-width node bay (two adjacent bays), 16 Gbps per lane. The four lanes support 4x10 Gbps (40 Gbps) or Fourteen Data Rate InfiniBand at 56 Gbps.
  - Four x1 ports or a single x4 port on each compute node
  - Up to 16 logical I/O modules (four per physical I/O module)
- One Flex System Manager management node, which provides multiple-chassis management support. Two Flex System Manager management nodes can be used for redundancy in a multiple-chassis configuration.
- Two Lenovo Flex System Chassis Management Modules (CMMs) for redundancy. A CMM provides single-chassis management support.

- Two fan logic modules, which detect fan module presence and provide a communication path to the fan modules.
- Two fan distribution cards, which pass the power and signals from the midplane to the fan modules and the fan logic modules.
- One rear LED card, which stores the vital product data (VPD) of the chassis components.

The chassis system provides the following features:

- **X-Architecture**

  The Flex System Enterprise Chassis is an X-Architecture system that uses proven innovative technologies to build powerful, scalable, and reliable compute node platforms. It provides features such as Predictive Failure Analysis (PFA) and real-time diagnostics.
- **Compute node expansion capabilities**You can install up to fourteen 1-bay compute nodes or seven 2-bay compute nodes in the chassis. Some compute nodes have connectors for additional optional devices that you can use to add capabilities to the compute nodes. For example, you can install optional I/O expansion adapters to add network interfaces or storage through the I/O modules.
- **Hot-swap capabilities**

  All component bays in the chassis are hot-swappable. For example, you can add, remove, or replace a compute node, I/O module, Flex System Manager management node, Chassis Management Module, fan logic module, fan module, or power supply without disconnecting the power from the chassis.
- **High-availability design**

  The following components in the chassis enable continued operation if one of the components fails:

  – **Power supplies**

    The power supplies support a single power domain that provides dc power to all of the chassis components. If a power supply fails, the other power supplies can continue to provide power. For power redundancy, additional power supplies can be installed.

    Note: The power management policy that you have implemented for the chassis determines the result of a power-supply failure.

  – **I/O modules**

    The I/O module bays provide a four-lane physical interface to each 1-bay compute node that supports speeds up to 56 Gbps. The I/O modules must be installed in pairs if you want them to be redundant.

  – **Fan modules**

    The fan modules provide cooling to all of the chassis components.

  – **Fan logic modules**

    The fan logic modules enable the Chassis Management Module to monitor the fans and control fan speed.
- **Chassis midplane**

  The chassis midplane provides the following features:

  – Redundant high-speed serialize/deserialize (SERDES) interconnects between compute nodes and I/O modules

  – I2C communication paths between the CMM and all devices in the chassis

  – 1 Gb Ethernet communication paths between the CMM and all compute nodes and I/O modules

  – Power distribution to all nodes and modules

  The midplane provides hot-swap connectors for the following components:

- Fourteen 1-bay compute nodes or seven 2-bay compute nodes
- Four I/O modules
- Two CMMs
- Six power supplies
- Ten fan modules
- Two fan logic modules

- **Systems management**

  If an Flex System Manager management node is installed, it provides configuration and management support for multiple chassis, their devices, and the compute nodes locally or remotely. You can install up to two management nodes in each multiple-chassis configuration (one management node each of in two of the chassis) for redundancy. This enables the system to continue to operate without disruption if one fails. The management node provides all of the management functions that the CMM provides, plus other advanced management functions. For more information about the Flex System Manager, see http://flexsystem.lenovofiles.com/help/index.jsp.

  The Lenovo Flex System Chassis Management Module (Chassis Management Module or CMM) provides single-chassis management. The Chassis Management Module is used to communicate with the system-management processor in each compute node to provide system monitoring, event recording, and alerts and to manage the chassis, its devices, and the compute nodes. The chassis supports up to two CMMs. If one CMM fails, the second CMM can detect its inactivity, activate itself, and take control of the system without any disruption. For more information about the CMM, see http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.cmm.doc/cmm_product_page.html.

Table 1 “Minimum chassis configuration” on page 3 shows the minimum component configuration that is required for the Flex System Enterprise Chassis to operate.

Table 1. Minimum chassis configuration

The minimum chassis configuration table is a two-column table that lists the minimum number of components that must be installed in the Flex System Enterprise Chassis. Column 1 identifies the components and the minimum number of each component required. Column 2 identifies the chassis bay where the components are installed.

Component	Bay
Two power supplies	Power-supply bays 1 and 4
Two 40 mm fan modules	Fan bays 5 and 10
Four 80 mm fan modules	Fan bays 1, 2, 6, and 7
Two fan logic modules	Fan logic bays 1 and 2
Flex System Manager (optional, one per chassis)	Node bay 1
One Chassis Management Module	CMM bay 1
One I/O module	I/O bay 1
One compute node	Node bays 2 - 14

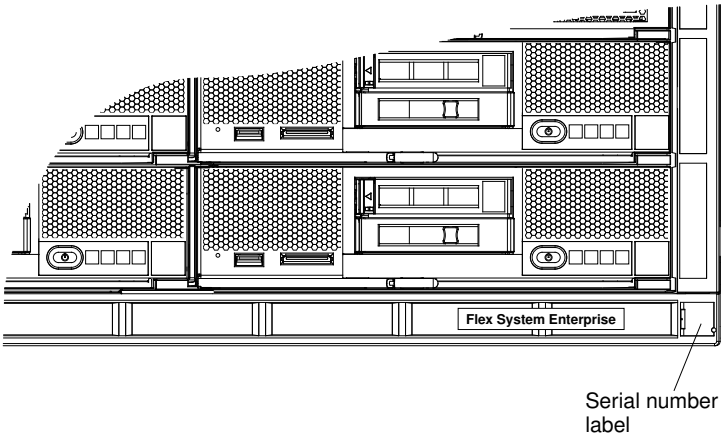
Record information about the Flex System Enterprise Chassis in Table 2 “Chassis reference information” on page 4. You will need this information for future reference.

Table 2. Chassis reference information

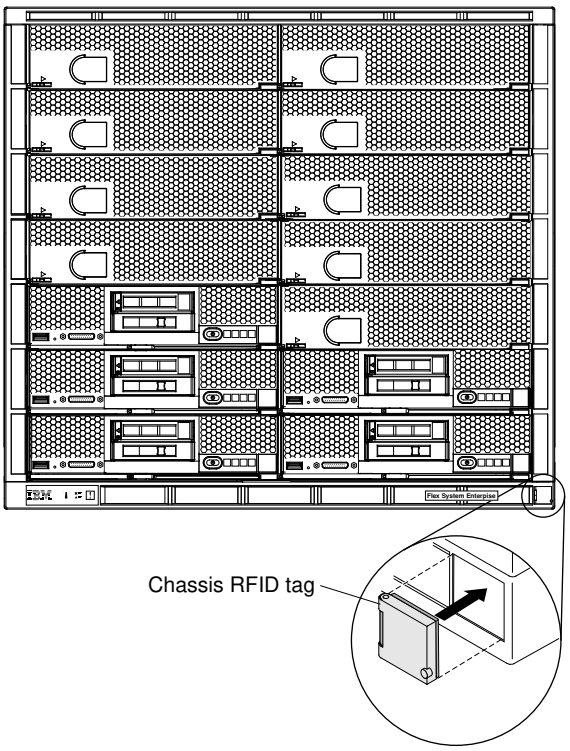
The chassis reference information table allows you to record the specific model number and serial number of your Flex System Enterprise Chassis.

Chassis reference information	
Product name	Flex System Enterprise Chassis
Machine type	7893, 8721, or 8724
Model number	_____
Serial number	_____

The serial number and model number are on the top, front, and rear of the chassis. The following illustration shows the location of the label on the front of the chassis.



If the chassis comes with an RFID tag, it is attached to the lower-right corner of the bezel. The following illustration shows the location of the RFID tag on the front of the chassis.



Related documentation

Use this information to identify and locate related chassis documentation.

This *Installation and Service Guide* contains general information about the Flex System Enterprise Chassis, including how to install and configure the chassis. It also contains information to help you solve problems yourself and instructions for removing and installing components, and it contains information for service technicians. The following documentation is also available:

- *Safety Information*

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

  This printed document contains the warranty terms and a pointer to the Lenovo Statement of Limited Warranty.
- *Environmental Notices and User Guide*

  This document is in PDF. It contains translated environmental notices.
- *License Agreement for Machine Code*

  This document is in PDF. It provides translated versions of the License Agreement for Machine code for your compute node.
- *Linux License Information and Attributions*

  This document is in PDF. It provides information about the open-source notices.
- *Chassis Management Module Command-Line Interface Reference Guide*

This document is in PDF. It explains how to use the Chassis Management Module command-line interface (CLI) to directly access chassis management functions. The command-line interface also provides access to the text-console command prompt on each compute node through a Serial over LAN (SOL) connection.

- *Chassis Management Module Installation Guide*

  This document is in PDF. It provides information about installing and configuring the Chassis Management Module.

To check for updated documentation, see http://flexsystem.lenovofiles.com/help/index.jsp.

Brocade documentation

Use this information to identify and locate related Brocade documentation.

The following section introduces Brocade documents that you might find useful for the installation and administration.

- **EN4023 User Guide**
  - *Network OS Layer 2 Switching Configuration Guide* - http://www.brocade.com/content/html/en/configuration-guide/nos-601a-l2guide/
  - *Network OS Command Reference Guide* - http://www.brocade.com/content/html/en/command-reference-guide/nos-601a-commandref/index.html
  - *Network OS Message Reference* - http://www.brocade.com/content/html/en/message-reference-guides/nos-601a-messageref/wwhelp/ wwhimpl/js/html/wwhelp.htm
- **FC5022 User Guide**
  - *Fabric OS Administrator's Guide* - http://www.brocade.com/content/html/en/administration-guide/fos-740-adminguide/
  - *Fabric OS Command Reference* - http://www.brocade.com/content/html/en/command-reference-guide/fos-741-commandref/wwhelp/ wwhimpl/js/html/wwhelp.htm
  - *Fabric OS Message Reference* - http://www.brocade.com/content/html/en/message-reference-guides/FOS_740_MESSAGES/wwhelp/ wwhimpl/js/html/wwhelp.htm#href=Title.1.2.html
  - *Access Gateway Administrator's Guide* - http://www.brocade.com/content/html/en/administration-guide/fos-740-accessgateway/index.html

The Lenovo Documentation CD

The documentation CD contains documentation for your Lenovo Flex System Enterprise Chassis Types 7893, 8721, and 8724 in Portable Document Format (PDF) and includes a documentation browser to help you find information quickly.

Hardware and software requirements

The Lenovo *Documentation* CD requires the following minimum hardware and software:

- MicrosoftWindows or Red Hat Linux
- 100 MHz microprocessor
- 32 MB RAM
- AdobeAcrobat Reader 3.0 (or later) or xpdf, which comes with Linux operating systems

Using the Documentation browser

Use the Documentation Browser to browse the contents of the CD, read brief descriptions of the documents, and view documents, using AdobeAcrobat Reader or xpdf. The Documentation Browser automatically

detects the regional settings in use in your system and presents the information in the language for that region (if available). If a topic is not available in the language for that region, the English-language version is displayed.

Use one of the following procedures to start the Documentation Browser:

- If Autostart is enabled, insert the CD into the DVD drive. The Documentation Browser starts automatically.
- If Autostart is disabled or is not enabled for all users:
  - If you are using a Windows operating system, insert the CD into the DVD drive, and click **Start → Run**. In the **Open** field, type: *e*:\win32.bat

    where *e* is the drive letter of your DVD drive, and click **OK**.
  - If you are using a Red Hat Linux, insert the CD into the DVD drive; then, run the following command from the /mnt/cdrom directory: sh runlinux.sh

Select your Flex System Enterprise Chassis from the **Product** menu. The **Available Topics** list displays all the documents for your product. Some documents might be in folders. A plus sign (+) indicates each folder or document that has additional topics under it. Click the plus sign to display the additional documents.

When you select a document, a description of the document appears under **Topic Description**. To select more than one document, press and hold the Ctrl key while you select the documents. Click **View Book** to view the selected document or documents in Acrobat Reader or xpdf. If you selected more than one document, all the selected documents are opened in Acrobat Reader or xpdf.

To search all the documents, type a word or word string in the **Search** field and click **Search**. The documents in which the word or word string appears are listed in order of the most occurrences. Click a document to view it, and press Ctrl+F to use the Acrobat search function, or press Alt+F to use the xpdf search function within the document.

Click **Help** for detailed information about using the Documentation Browser.

Notices and statements in this document

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

The following notices and statements are used in this document:

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

Features and specifications

This topic provides a summary of the specifications of the chassis.

The features and specifications table is a two-column table where each column lists the features and specifications of the Lenovo Flex System Enterprise Chassis Types 7893, 8721, and 8724.

Size (10U)

- Height: 440 mm (17.32 in.)
- Depth: 830 mm (32.68 in.)
- Width: 447 mm (17.6 in.)
- Weight:
  - Fully configured (stand-alone): approximately 220.4 kg (486.1 lb)
  - Fully configured (in the rack): approximately 225.6 kg (497.4 lb)
  - Empty chassis with shelves: approximately 65.7 kg (145 lb)
  - Empty chassis without shelves: approximately 44.4 kg (98 lb)

Node bays (front)

The chassis comes with fourteen node bays on the front that can physically contain the following:

- Up to fourteen 1-bay compute nodes.

  Note: The exact maximal number of supported 1-bay nodes is determined by input voltage and power redundancy policy. See the following table for detailed combinations, or alternatively, refer to https://datacentersupport.lenovo.com/us/en/products/solutions-and-software/software/lenovo-capacity-planner/solutions/ht504651 for more details.

  See the following tables for limited maximal number of different nodes that are supported in the same chassis.

Table 3. Limited maximal number of SN550 in the same chassis

	2500 W power output (200-208 V ac)			2745 W power output (200 or higher V ac)
Processor TDP	**N+1 N=3 4 PSUs with throttling**	**N+N N=3 6 PSUs with throttling**	**N+N N=3 6 PSUs without throttling**	**N+N N=3 6 PSUs without throttling**
85 W	**14**	**14**	**12**	**13**
105 W	**14**	**14**	**11**	**12**
125 W	**14**	**14**	**10**	**11**
130 W	**14**	**14**	**10**	**11**
140 W	**13**	**14**	**9**	**10**
150 W	**13**	**14**	**9**	**10**
165 W	**12**	**13**	**8**	**9**

Table 4. Limited maximal number of SN550 V2 in the same chassis

	2500 W power output (200-208 V ac)				
Processor TDP	**N+1 N=4 5 PSUs With throttle**	**N+1 N=3 4 PSUs With throttle**	**N+N N=3 6 PSUs With throttle**	**N+1 N=5 6 PSUs No throttle**	**N+N N=3 6 PSUs No throttle**
105 W	**14**	**14**	**14**	**14**	**9**
120 W	**14**	**13**	**14**	**14**	**8**
135 W	**14**	**12**	**13**	**13**	**8**
140 W	**14**	**12**	**13**	**13**	**8**
150 W	**14**	**12**	**12**	**12**	**7**
165 W	**14**	**11**	**11**	**12**	**7**
185 W	**13**	**10**	**10**	**11**	**6**
195 W	**13**	**9**	**9**	**10**	**6**
205 W	**13**	**9**	**9**	**10**	**6**
230W	**12**	**9**	**9**	**9**	**5**
	2745 W power output (220-240 V ac)				
Processor TDP	**N+1 N=4 5 PSUs With throttle**	**N+1 N=3 4 PSUs With throttle**	**N+N N=3 6 PSUs With throttle**	**N+1 N=5 6 PSUs No throttle**	**N+N N=3 6 PSUs No throttle**
105 W	**14**	**14**	**14**	**14**	**10**
120 W	**14**	**13**	**14**	**14**	**9**
135 W	**14**	**12**	**13**	**14**	**9**
140 W	**14**	**12**	**13**	**14**	**9**
150 W	**14**	**12**	**12**	**13**	**8**
165 W	**14**	**11**	**11**	**13**	**8**
185 W	**14**	**11**	**11**	**12**	**7**
195 W	**14**	**10**	**10**	**11**	**6**
205 W	**14**	**10**	**10**	**11**	**6**
230W	**13**	**9**	**9**	**10**	**6**

- Up to seven 2-bay compute nodes (with the shelves removed from the chassis)
- Up to three 4-bay storage nodes or enclosures (with the shelves removed from the chassis)
- Mixing of 1-bay, 2-bay and 4-bay nodes (with the shelves removed from the chassis)

Device capacity (rear)

The chassis comes with the following bays on the rear:

- Two hot-swap Chassis Management Module bays
- Six hot-swap power-supply bays
- Ten hot-swap fan bays
- Four hot-swap I/O bays
- Two hot-swap fan logic bays

Upgradeable microcode

Microcode is upgradeable when fixes or features are added.

- Flex System Manager management node firmware
- Chassis Management Module firmware
- I/O module firmware
- Compute node firmware

Security features

- Login password for remote connection
- Secure Sockets Layer (SSL) security for remote management access
- Lightweight Directory Access Protocol (LDAP)
- Trusted and signed firmware

Predictive Failure Analysis (PFA) alerts

- Power supplies
- Node dependent features

Electrical input

- Rated voltage and frequency 200 - 240 V ac single phase at 47-63 Hz
- Inrush current (chassis maximum) 40 A
- Leakage current (chassis maximum) 580 uA
- Branch circuit breaker 20 A maximum

Power supplies

- Minimum: Two hot-swap power supplies
- Maximum: Six hot-swap power supplies
- Available with 2100 Watt or 2500 Watt, 200 - 240 V ac power supplies (IEC 60320 type C20 line cord connector)
- Available in certain markets with 2500 Watt, 240 - 380 V dc power supplies (RF-203 line cord connector)
- Optional 2500 Watt, -48 to -60 V dc power supplies (2 position power connector)

Fan

Up to 10 variable-speed, hot-swap fan modules are supported, including the following:

- Two 40 mm fan modules
- Up to eight 80 mm fan modules

Management modules

Two hot-swap Chassis Management Modules

I/O modules

Supports up to four scalable switch modules with each providing a 4-lane physical interconnect.

Heat output

- **Approximate heat output:**
  - Minimum configuration: 1365 Btu per hour (400 watts)
  - Maximum configuration: 44,017 Btu per hour (12,900 watts)
- **Declared sound power level:** 7.5 bels
- **Chassis airflow:** Full chassis configuration with all nodes, I/O modules, power supplies, and fan modules installed.
  - Minimum - 270 CFM
  - Maximum - 1,020 CFM

Environment:

The Flex System Enterprise Chassis complies with ASHRAE class A3 specifications.

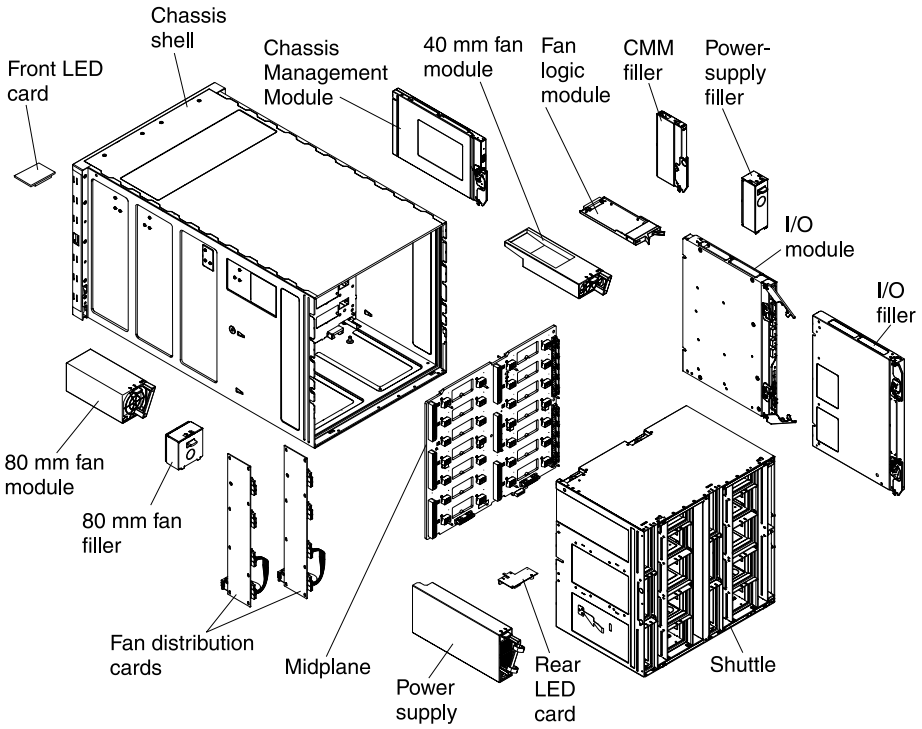
- Power on [1]:
  - Temperature: 5°C - 40°C (41°F - 104°F) [3]
  - Humidity, non-condensing: -12°C dew point (10.4°F) and 8% - 85% relative humidity [5,6]
  - Maximum dew point: 24°C (75°F)
  - Maximum altitude: 3048 m (10,000 ft)
  - Maximum rate of temperature change: 5°C/hr (41°F/hr) [4]
- Power off [2]:
  - Temperature: 5°C to 45°C (41°F - 113°F)
  - Relative humidity: 8% - 85%
  - Maximum dew point: 27°C (80.6°F)
- Storage (non-operating):
  - Temperature: 1°C to 60°C (33.8°F - 140°F)
  - Altitude: 3050 m (10,006 ft)
  - Relative humidity: 5% - 80%
  - Maximum dew point: 29°C (84.2°F)
- Shipment (non-operating) [3]:
  - Temperature: -40°C to 60°C (-40°F - 140°F)
  - Altitude: 10,700 m (35,105 ft)
  - Relative humidity: 5% - 100%
  - Maximum dew point: 29°C (84.2°F) [8]

1. Chassis is powered on.
2. Chassis is removed from original shipping container and is installed but not in use, for example, during repair, maintenance, or upgrade.
3. The equipment acclimation period is 1 hour per 20°C of temperature change from the shipping environment to the operating environment.

Major chassis components

The major components in the Flex System Enterprise Chassis include an Flex System Manager management node, compute nodes, I/O modules, power supplies, fan modules, fan distribution cards, fan logic modules, the front panel LED card, and the rear LED card.

The following illustration shows the major components in the Flex System Enterprise Chassis:

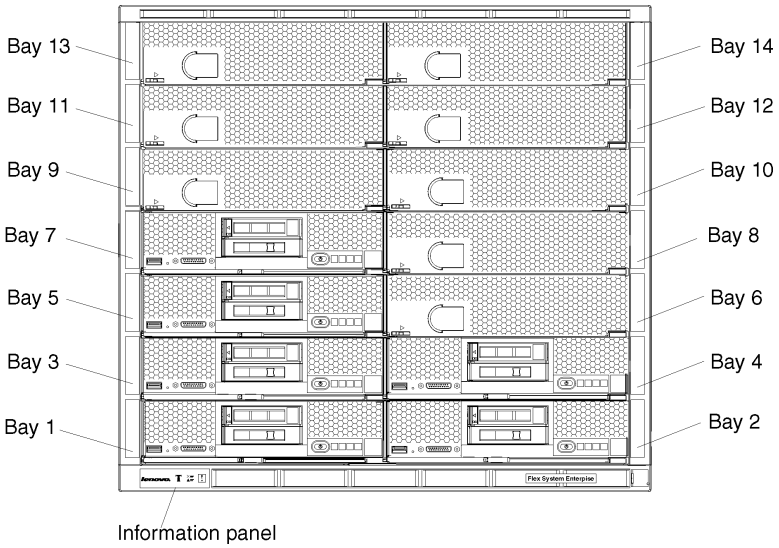


Front view of the Flex System Enterprise Chassis

Compute nodes, the Flex System Manager management node, and the front panel LED card are in the front of the Flex System Enterprise Chassis.

Note: For proper cooling, each bay in the chassis must contain either a device or a filler.

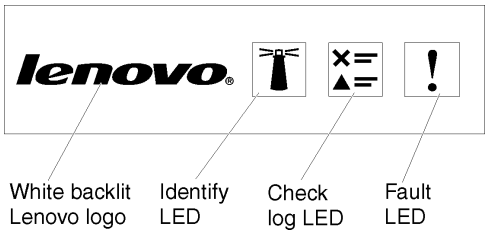
The following illustration shows the front of the chassis.



Front information panel

The Flex System Enterprise Chassis has LEDs on the front information panel that you can use to obtain the status of the chassis.

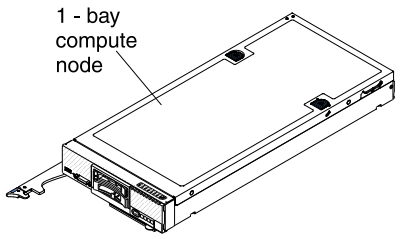
The following illustration shows the chassis front information panel LEDs. The Identify, Check log, and Fault LEDs on the chassis front panel are also visible on the rear of the chassis. For more information about using the chassis front information panel LEDs, see “Front information panel LEDs” on page 926.

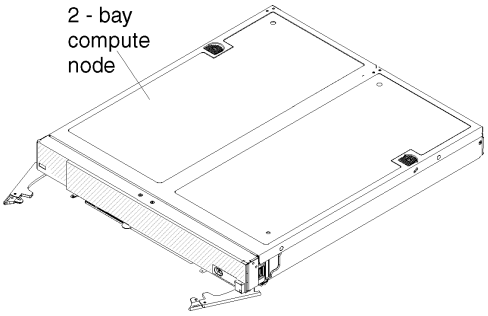


Compute nodes

Compute nodes contain components such as microprocessors, memory, Ethernet controllers, and hard disk drives. They receive power and network connections from the Flex System Enterprise Chassis.

The Flex System Enterprise Chassis supports up to fourteen 1-bay compute nodes or up to seven 2-bay compute nodes when the chassis shelves are removed.





For more information about the compute nodes that are available for the Flex System Enterprise Chassis, see http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.common.nav.doc/compute_blades.html.

To determine which compute nodes are compatible with the Flex System Enterprise Chassis, see http://www.lenovo.com/serverproven/.

Storage nodes

Storage nodes include control modules and disk drives. They receive power and network connections from the Flex System Enterprise Chassis.

An Flex System storage node consists of a storage control enclosure mounted in an Flex System Enterprise Chassis. Each storage node might also include one or more storage expansion enclosures.

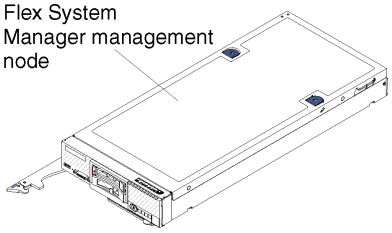
See http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.4939.doc/site_product_page.html for more information about the storage nodes that are available for the Flex System Enterprise Chassis.

Note: A 4-bay storage control enclosure or expansion enclosure occupies four adjacent node bays (two vertically and horizontally) in the chassis and requires the chassis shelves and shelf supports to be removed prior to installation.

Flex System Manager management node

The Flex System Manager management node is a platform management appliance that you can use to configure and manage multiple chassis platforms remotely.

The Flex System Manager management node provides systems-management functions for all compute nodes in a multiple-chassis configuration. The management node can be installed in any node bay.



The Flex System Enterprise Chassis supports up to two management nodes in a multiple-chassis configuration, and a management node can be installed in any node bay.

Note:

- You can install up to two management nodes in a multiple-chassis configuration for redundancy (one management node in two of the chassis). This enables the system to continue to operate without disruption if one fails.

- When you install a second management node in a multiple-chassis configuration, make sure that it is installed in a different node bay than the first management node in the first chassis. For example, if the first management node is in node bay 1 of the first chassis, then the second management node must be in a node bay other than node bay 1 in a different chassis.
- The management nodes default static IP address depends in part on the node bay that it is installed in. If you install two management nodes in the same node bay in different chassis in a multiple-chassis configuration, they will have the same default IP address.
- In a configuration with two management nodes, configure one management node and bring it up before you configure the second management node.

The Flex System Manager management node provides the following features and functions:

- Active-passive node failover (optional feature)
- Basic life-cycle management of all chassis components:
  - Configuration, diagnostics, health, alerts, and updates
  - Multiple-chassis management (optional feature)
  - Network manager
  - Service and support manager
- Service data collection
- Security (single sign-on, audit logging, role based access control, user management)
- Advanced managers:
  - Active Energy Manager
  - Network control
  - Security control
  - Storage control
  - VMcontrol - Enterprise (optional feature)

The Service and Support Manager function of the Flex System Manager automatically detects serviceable hardware problems and collects supporting data for serviceable hardware problems that occur on your monitored systems.

The Electronic Service Agent tool is integrated with Service and Support Manager and transmits serviceable hardware problems and associated support files to Support.

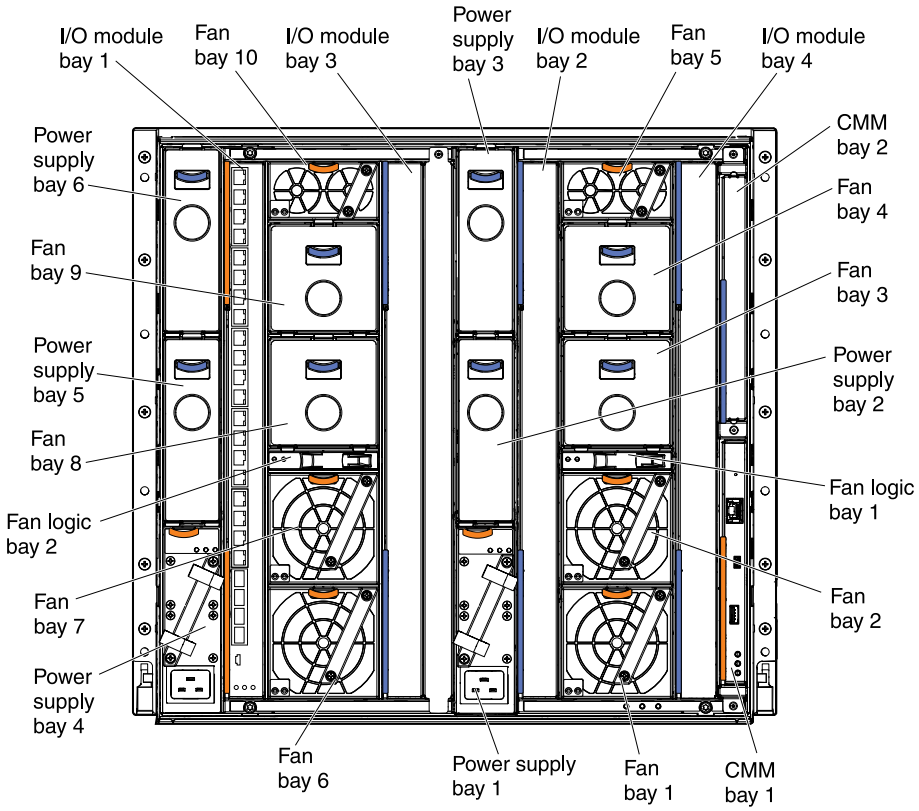
For more information about the Flex System Manager, see http://flexsystem.lenovofiles.com/help/index.jsp.

Rear view of the chassis

Fan modules, I/O modules, power supplies, fan logic modules, and the Lenovo Flex System Chassis Management Modules are in the rear of the Flex System Enterprise Chassis.

Note: Each bay in the chassis must contain either a device or a filler.

The following illustration shows the rear view of the chassis.



Flex System Chassis Management Module

The Lenovo Flex System Chassis Management Module (Chassis Management Module or CMM) is a hot-swap module that configures and manages all installed chassis components. The chassis comes with one Chassis Management Module in the CMM bays.

The Chassis Management Module provides the communication link with a compute node system-management processor (also called the integrated management module). It supports compute node features such as power-on requests, error and event reporting.

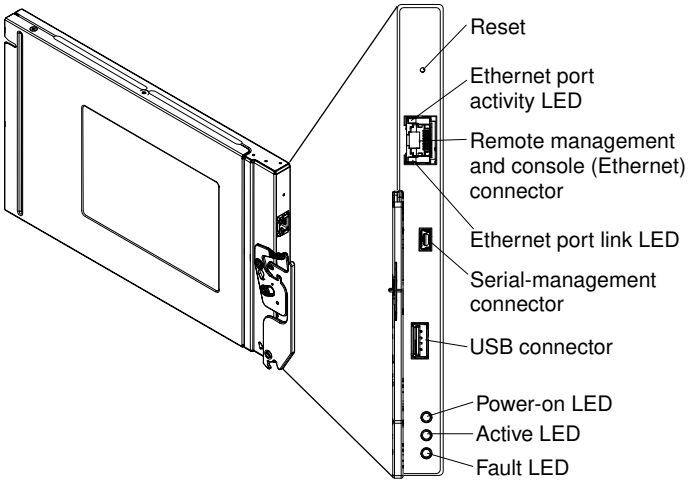
The CMM provides the following features and functions:

- Single-chassis management
- Power control and fan management
- Chassis and compute node initialization
- Chassis management network
- Diagnostics
- Service data collection and call home services
- Resource discovery and inventory management
- Resource alerts and monitoring management
- Chassis and compute node power management
- Network management

The Chassis Management Module provides systems-management functions. It contains the following connections:

- A serial management connector (mini-USB form factor) for a local connection to another computer, such as a notebook computer
- An external standard USB connector (future use)
- A 10/100/1000 Mbps remote management and console (Ethernet) connector

The following is an illustration of the Chassis Management Module:

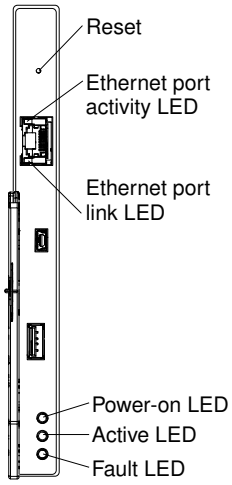


The chassis supports up to two Chassis Management Modules, and they must be installed in the CMM bays.

For more information about the Lenovo Flex System Chassis Management Module, see http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.cmm.doc/cmm_product_page.html.

CMM controls and indicators

The Flex System Chassis Management Module (CMM) has LEDs and controls that you can use to obtain status information and restart the CMM.



The CMM has the following LEDs and controls:

Reset button

Use this button to restart the Chassis Management Module. Insert a straightened paper clip into the reset button pinhole; then, press and hold the button in for at least one second to restart the CMM. The

restart process initiates upon release of the reset button but might not be immediately apparent in some cases.

Attention: If you press the reset button, hold it for at least 10 seconds, then release it, the CMM will restart and reset back to the factory default configuration. Be sure to save your current configuration before you reset the CMM back to factory defaults. The combined reset and restart process initiates upon release of the reset button but might not be immediately apparent in some cases.

Note: Both the CMM restart and reset to factory default processes require a short period of time to complete.

Power-on LED

When this LED is lit (green), it indicates that the CMM has power.

Active LED

When this LED is lit (green), it indicates that the CMM is actively controlling the chassis.

Only one CMM actively controls the chassis. If two CMMs are installed in the chassis, this LED is lit on only one CMM.

Fault LED

When this LED is lit (yellow), an error has been detected in the CMM. When the error LED is lit, the chassis fault LED is also lit.

Ethernet port link (RJ-45) LED

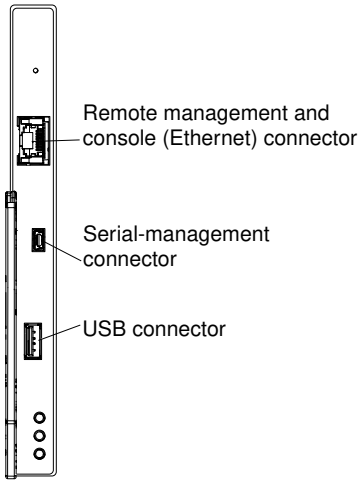
When this LED is lit (green), it indicates that there is an active connection through the remote management and console (Ethernet) port to the management network.

Ethernet port activity (RJ-45) LED

When this LED is flashing (green), it indicates that there is activity through the remote management and console (Ethernet) port over the management network.

CMM input and output connectors

The Flex System Chassis Management Module provides one serial connector (mini-USB) and one Ethernet connector for remote management and one standard USB connector.



Remote management and console (Ethernet) connector

The remote management and console connector (RJ-45) is the management network connector for all chassis components. This 10/100/1000 base T Ethernet connector is usually connected to the management network through a top-of-rack switch. During the initial setup of an optional management node, the system console is connected to the top-of-rack switch that is connected to this Ethernet port.

Serial-management connector

The serial-management connector (RS-232, mini-USB form factor) is used to connect the CMM to a management device, through a serial cable or serial management network, to manage the chassis. This connector provides local access for the CMM to the Serial over LAN (SOL) interface of any compute node. For example, you can connect a notebook computer to the serial-management connector and use a terminal emulator program to configure the IP addresses, user accounts, and other settings.

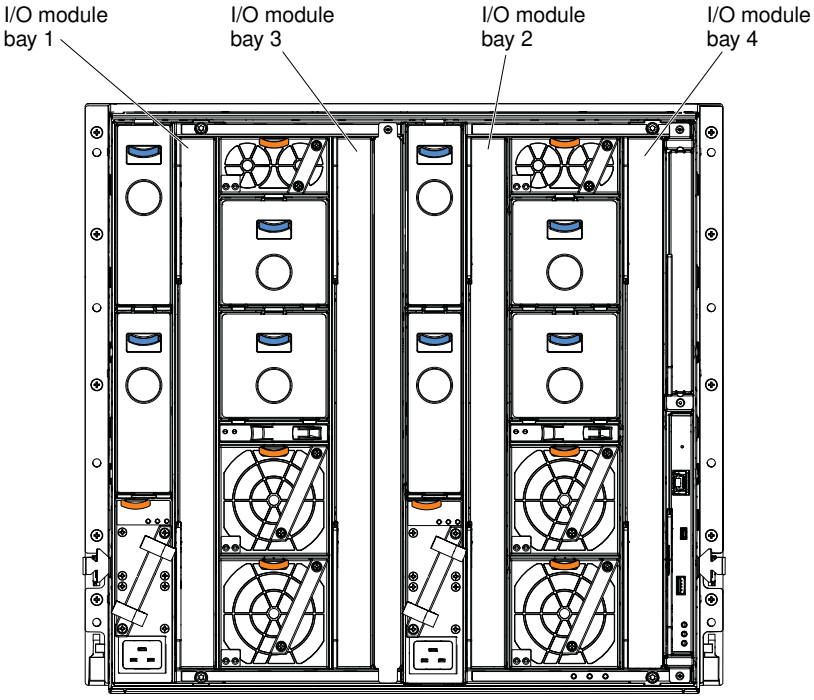
USB connector

This is a standard USB connector (future use).

I/O modules

You can install up to four I/O modules in the Flex System Enterprise Chassis, including Ethernet switch modules, Fibre Channel switch modules, Infiniband, and pass-thru modules (optical and copper).

The following is an illustration that shows the chassis I/O bays.



Note:

I/O modules all have fault and power-on LEDs similar to those found on the other chassis components. I/O modules also have connectors that are unique to the device.

- For more information about the I/O modules that are available for the Flex System Enterprise Chassis, see http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.networkdevices.doc/network.html.
- To determine which I/O modules are compatible with the Flex System Enterprise Chassis, see http://www.lenovo.com/serverproven/.

I/O module bays 1 and 2

I/O module bays 1 and 2 support Ethernet switches or pass-thru modules. These I/O bays connect to Ethernet ports 0 and 1 on the nodes installed in node bays 1 through 14. Most compute nodes feature two integrated Ethernet ports; for nodes without integrated Ethernet ports, an Ethernet expansion adapter must be installed in the I/O expansion port 1 connector of the node. See the documentation that comes with the node for more information about connecting it to the I/O modules in I/O bays 1 and 2.

I/O module bays 3 and 4

The I/O module bays 3 and 4 support optical and copper I/O modules such as Ethernet, Fibre Channel, and Infiniband switches, and pass-thru modules. To connect a node to a module in I/O bays 3 or 4, an expansion adapter that supports the I/O module is required. See the documentation that comes with the node for more information about connecting it to the I/O modules in I/O bays 3 and 4.

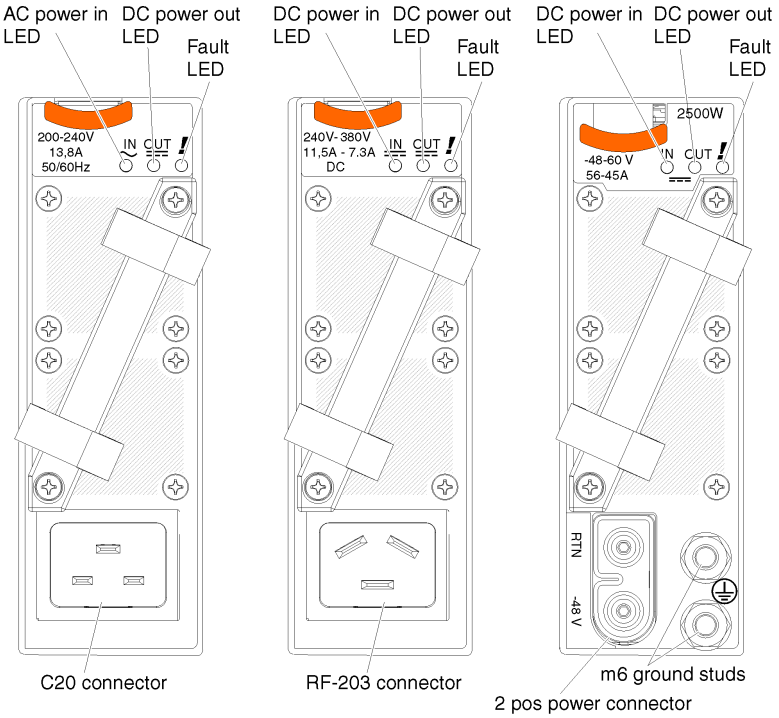
Power supplies

The Flex System Enterprise Chassis supports up to six autoranging power supplies.

The types of power supplies that are available for the Flex System Enterprise Chassis are listed in Table 5 “Chassis power supplies” on page 20.

Table 5. Chassis power supplies

Rated output	Input voltage range	Power cord connector	FRU numbers
2100 W	200 to 240 V ac	C20	94Y8253 or 69Y5892
2500 W	200 to 240 V ac	C20	94Y8251 or 69Y5890
2500 W	240 to 380 V dc[1]	RF-203	94Y8274
2500 W	-48 to -60 V dc	2 position power connector	94Y8265
1. Tolerance 192 - 400 V dc.			



200-240 V ac power supply **240-380 V dc power supply** **-48 to -60 V dc power supply**

The power supplies get electrical power from either a 200 to 240 V ac power source, a 240 to 380 V dc power source, or a -48 to -60 V dc power source depending on the type of power supply. Both ac and dc-powered supplies convert the power source into 12 V dc and 3.3 V dc outputs to the system midplane. The power supplies are capable of autoranging within the input voltage range. There is one common power domain for the chassis that distributes dc power to each of the nodes and modules through the system midplane.

Power supply redundancy is achieved when there is one more power supply available than is needed to provide full power to all chassis components. Power source redundancy is achieved by distributing the power cord connections between independent supply circuits. See “Connecting the chassis to power” on page 55 for more information.

Each power supply has internal fans and a controller. The power supply controller can be powered by any installed power supply that is providing dc power through the midplane. The power supply does not have to be connected to a power source to communicate with the CMM, as long as dc power is available from the midplane.

Attention: The power supplies contain internal cooling fans. Do not obstruct the fan exhaust vents.

Up to six power supplies can be installed. The number of power supplies that you install is dependent on the type of power supply, the chassis power load, and selected chassis power policy.

Important: Do not mix different types of power supplies in the Flex System Enterprise Chassis.

- Mixing ac-powered supplies with dc-powered supplies in the same chassis is not supported. Each chassis must contain either all ac-powered supplies or all dc-powered supplies.
- For ac-powered chassis, do not mix 2100 W and 2500 W power supplies. Chassis powered by ac power should contain only power supplies of the same wattage.
- For dc-powered chassis, do not mix 240 to 380 V dc and -48 to -60 V dc power supplies. Chassis powered by dc power should contain only power supplies of the same input voltage.

For example, if a 2100 W power supply is installed in a chassis containing 2500 W power supplies, the CMM will budget power as if all of the power supplies are 2100 W. In this scenario, the Fault LED on the mismatched power supply and the chassis Fault LED are lit and a warning message is sent to the CMM event log. In addition, if the chassis power budget is insufficient, the CMM might not allow all of the devices in the chassis to power on.

Note:

- 200 - 208 VAC, 3-Phase Delta power distribution units (PDUs): The power supplies are designed so that three power supplies will consume the power of and balance the phases of a 30 A, 3-phase PDU; or six power supplies will consume the power of and balance the phases of a 60 A, 3-phase PDU.
- 380 - 450 VAC, 3-Phase Y PDU: The power supplies are designed so that three power supplies will nearly consume the power of and balance the phases of a 16A, 3-phase PDU, or six power supplies will nearly consume the power of and balance the phases of a 32 A, 3-phase PDU.
- Single-phase PDUs can be used, however, the building power service may be unbalanced and the PDU power may not be fully utilized.

Power supply controls and indicators

There are three LEDs on each power supply:

AC power in LED (200 - 240 V ac supplies only)

When this LED is lit (green), it indicates that ac power is being supplied to the power supply.

DC power in LED (240 to 380 and -48 to -60 V dc supplies)

When this LED is lit (green), it indicates that dc power is being supplied to the power supply.

DC power out LED

OUT

When this LED is lit (green), it indicates that dc power is being supplied from the power supply to the chassis midplane.

Fault LED

!

When this LED is lit (yellow), it indicates that there is a fault with the power supply.

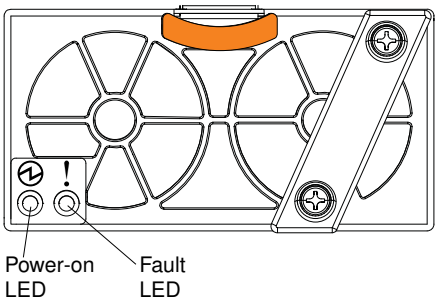
Note: Before unplugging the ac power cord from the power supply or removing the power supply from the chassis, verify that the capacity of the remaining power supplies are sufficient to meet the minimum power requirements for all components in the chassis. You can view the power status and requirements through the Flex System Manager. For information on accessing and using the Flex System Manager, see http://flexsystem.lenovofiles.com/help/index.jsp.

Fan modules

The Flex System Enterprise Chassis supports up to ten fan modules (two 40 mm fan modules and eight 80 mm fan modules). It comes with a minimum of six hot-swap fan modules installed (four 80 mm fan modules and two 40 mm fan modules).

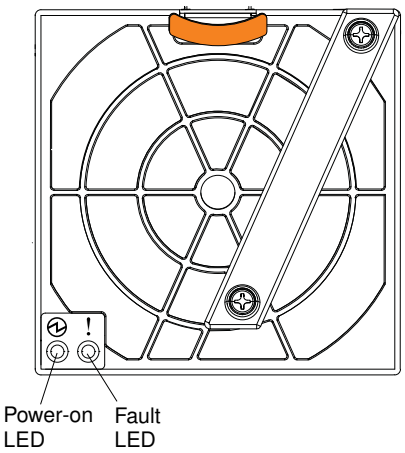
40 mm fan modules

The two smaller 40 mm fan modules at the top of the chassis provide cooling to the I/O modules and the CMMs. The following is an illustration of the 40 mm fan modules:



80 mm fan modules

The larger 80 mm fan modules provide cooling to the compute nodes and the Flex System Manager management node, if one is installed. The following is an illustration of the 80 mm fan modules:



The following 80 mm fan modules are available for the Flex System Enterprise Chassis.

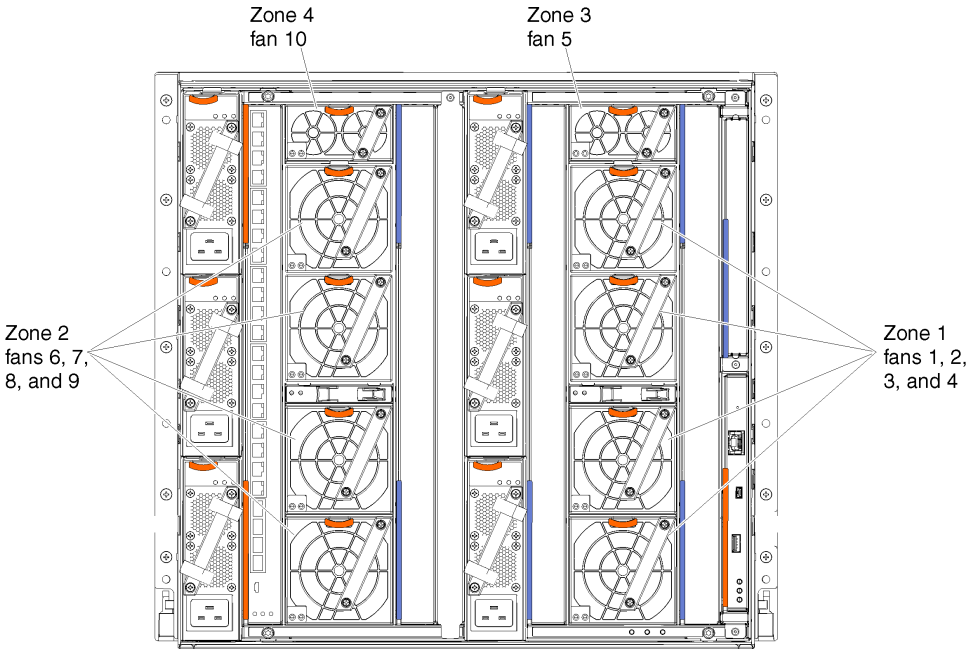
Fan type	Part number	Application
80 mm, single fan	TBD	Flex System Enterprise Chassis equipped with 2100 watt power supplies
80 mm, dual fan	81Y2910	Flex System Enterprise Chassis equipped with 2500 watt power supplies

Attention: Do not mix single-fan and dual-fan 80 mm fan modules within an Flex System Enterprise Chassis. Use only the type of 80 mm fan module indicated for your machine type.

Note: Not all of the 80 mm fan modules are required. Empty 80 mm fan bays must have a filler installed to maintain adequate cooling. See “Installing components” on page 41 to determine the number of 80 mm fan modules required and where they should be installed in your configuration.

Fan zones

Compute node cooling is logically split between the left and right half of the chassis. The ten fan modules provide cooling in four zones as shown in the following illustration:



- Zone 1 includes four 80 mm fan modules numbered 1, 2, 3, and 4 on the right rear of the chassis. Zone 1 fans provide cooling for the odd-numbered node bays (1, 3, 5, 7, 9, 11, and 13) on the left front of the chassis. These fans provide airflow to the nodes directly in front of them.
- Zone 2 contains four 80 mm fan modules numbered 6, 7, 8, and 9 on the left rear of the chassis. Zone 2 fans provide cooling for the even-numbered node bays (2, 4, 6, 8, 10, 12, and 14) on the right front of the chassis. These fans provide airflow to the nodes directly in front of them.
- Zone 3 contains one 40 mm fan module (fan 5) on the top right rear of the chassis. Fan 5 provides cooling for I/O modules 2 and 4 as well as both CMMs on the right rear side of the chassis.
- Zone 4 contains one 40 mm fan module (fan 10) on the top left rear of the chassis. Fan 10 provides cooling for I/O modules 1 and 3 on the left rear side of the chassis.

Fan module controls and indicators

The fan modules have two LEDs:

Power-on LED

When this LED is lit (green), it indicates that the fan module has power.

Fault LED

When this LED is lit (yellow), it indicates that the fan module has failed.

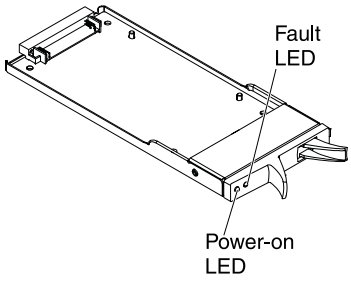
Fan logic modules

The Flex System Enterprise Chassis comes with two installed hot-swap fan logic modules.

The fan logic modules allow the Chassis Management Module to monitor the chassis fans. The fan logic modules must be installed in order for the Chassis Management Module to communicate with the fan modules and monitor fan presence, fan speed, and fan failures.

There is one fan logic module for each side of the chassis and it only allows communication to the fan modules on the same side of the chassis. You can replace a fan logic module without shutting down the chassis. The fans will not be monitored while the fan logic module is removed.

The following is an illustration of the fan logic module:



Fan logic module controls and indicators

The fan logic modules have two LEDs:

Power-on LED
When this LED is lit (green), it indicates that the fan logic module has power.

Fault LED
When this LED is lit (yellow), it indicates that the fan logic module has failed.

Chapter 2. Installing the Flex System Enterprise Chassis

Install the Flex System Enterprise Chassis in your facility by setting up and configuring all of the hardware components.

Before you begin the installation process, make sure that you have completed all planning activities. Planning information is available from http://flexsystem.lenovofiles.com/help/index.jsp.

Setting up your Flex System Enterprise Chassis

Follow the instructions in this section to set up the Flex System Enterprise Chassis hardware.

Before you begin, make the following preparations:

- Read “Safety” on page iii and “Handling static-sensitive devices” on page 958. This information will help you work safely.
- Confirm that each box contains all the components that are listed on the packing list. Your order might consist of more than one box, and each box might contain more than one component.
- Make sure that at least 10 units of contiguous space (10U) is available in the rack.

To set up the chassis hardware, complete the following tasks:

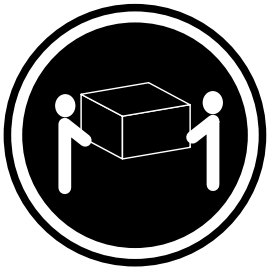
1. Remove the components from the chassis to decrease the weight so that it can be safely installed in the rack (see “Removing components” on page 27). You can also remove the chassis shelves to further reduce the weight. You do not have to remove the two fan logic modules in the rear of the chassis.
2. Install the chassis in a rack (see “Installing the chassis in a rack” on page 33).
3. Reinstall all of the components that you removed (see “Installing components” on page 41).
4. Cable the components in the chassis to the applicable external devices (see “Cabling the chassis” on page 54).
5. Connect the chassis to power (see “Connecting the chassis to power” on page 55).

Note: The Flex System Enterprise Chassis does not have a power switch. To turn off chassis power, see “Disconnecting the chassis from power” on page 60.

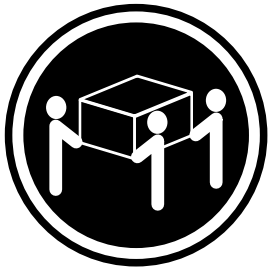
Removing components

Remove components to reduce the weight of the Flex System Enterprise Chassis so that it can safely be installed in the rack.

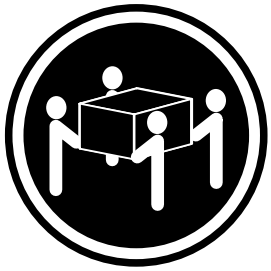
Statement 4



≥ 18 kg (39.7 lb)



≥ 32 kg (70.5 lb)

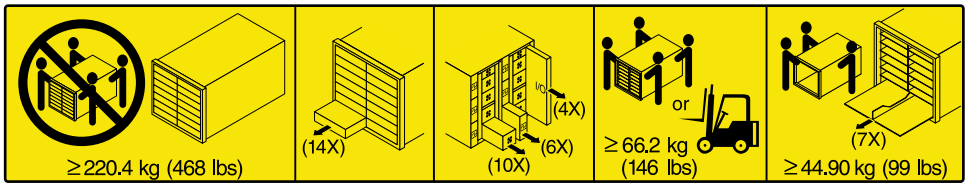


≥ 55 kg (121.2 lb)

CAUTION:
Use safe practices when lifting.

Statement 32

CAUTION:
To avoid personal injury, before lifting the unit, remove all the blades, power supplies, and removable modules to reduce the weight.

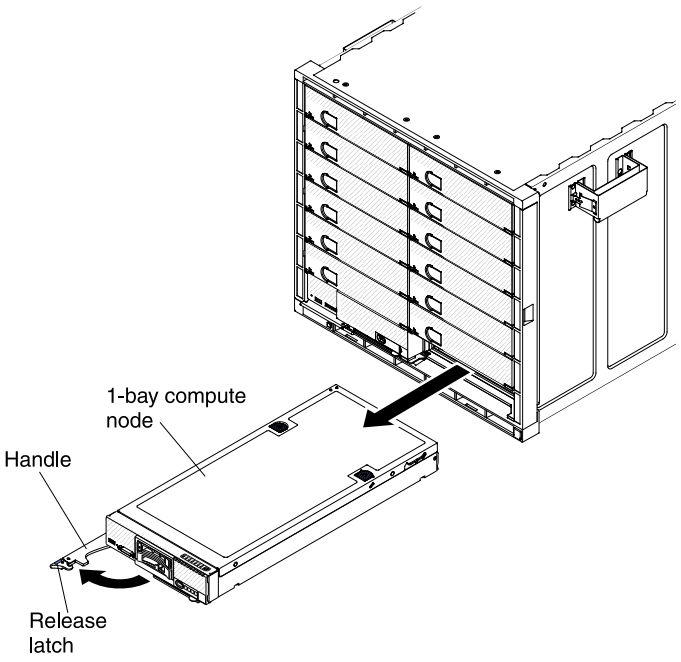


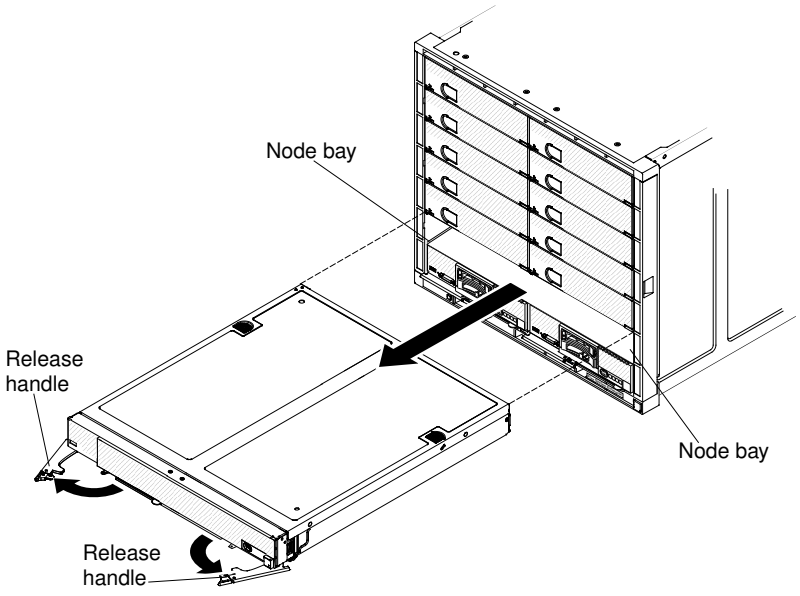
Complete the following steps:

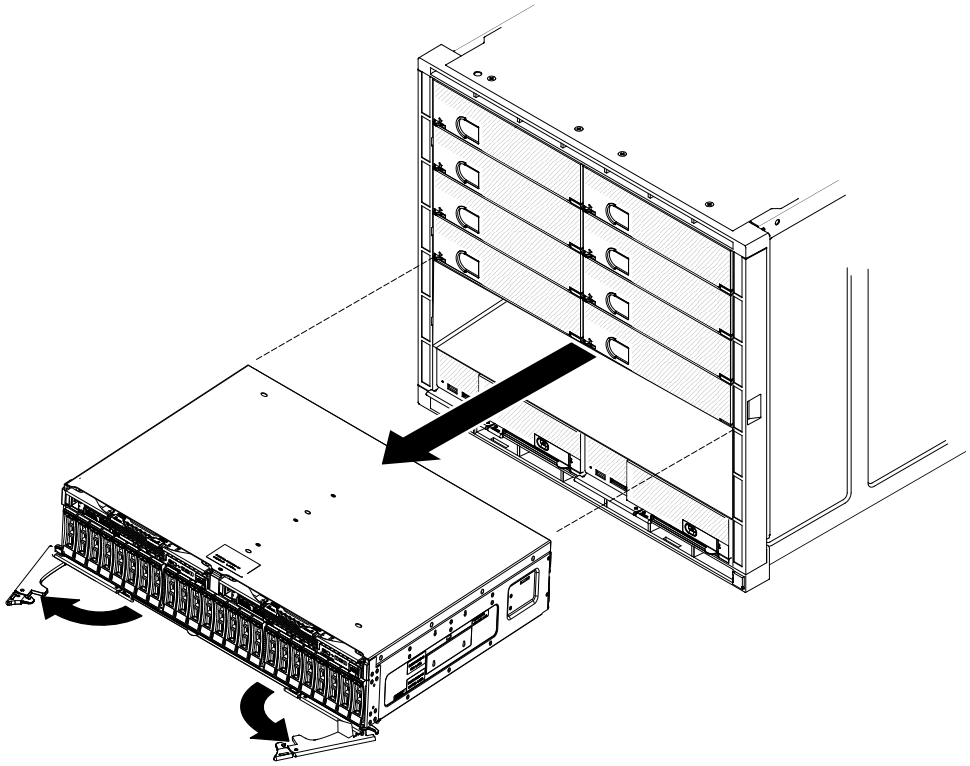
Step 1. Remove the components from the front of the chassis and place them on a flat, static-protective surface.

a. Read “Safety” on page iii and “Handling static-sensitive devices” on page 958.

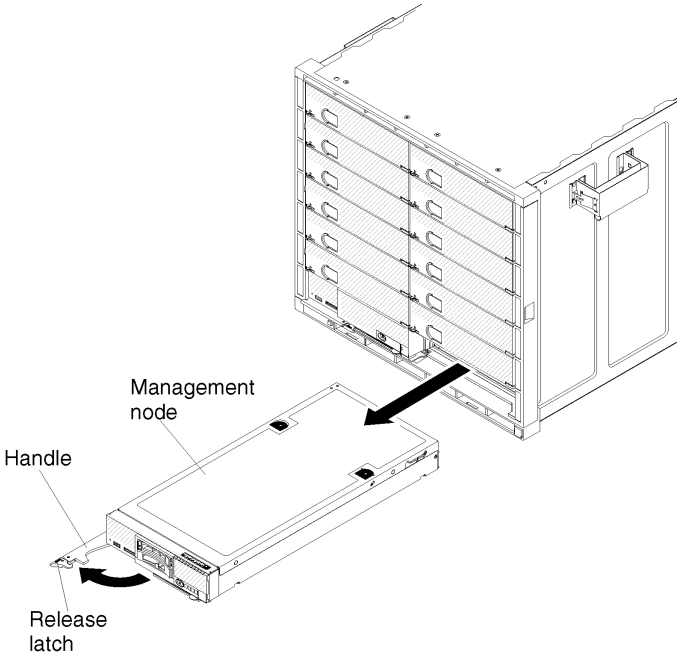
b. Remove all of the installed compute nodes or storage nodes.


1-bay compute node
Handle
Release latch


Node bay
Release handle
Node bay
Release handle



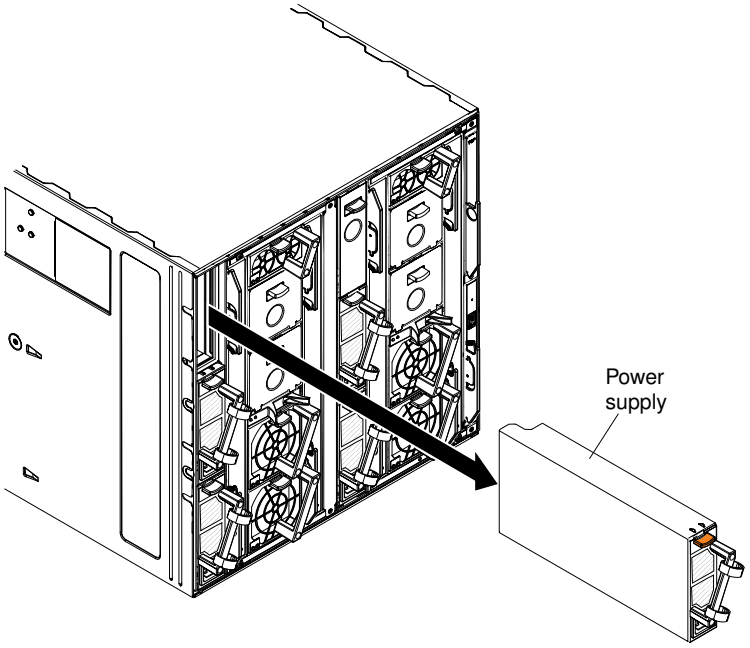
c. Remove the Flex System Manager management node, if one is installed.



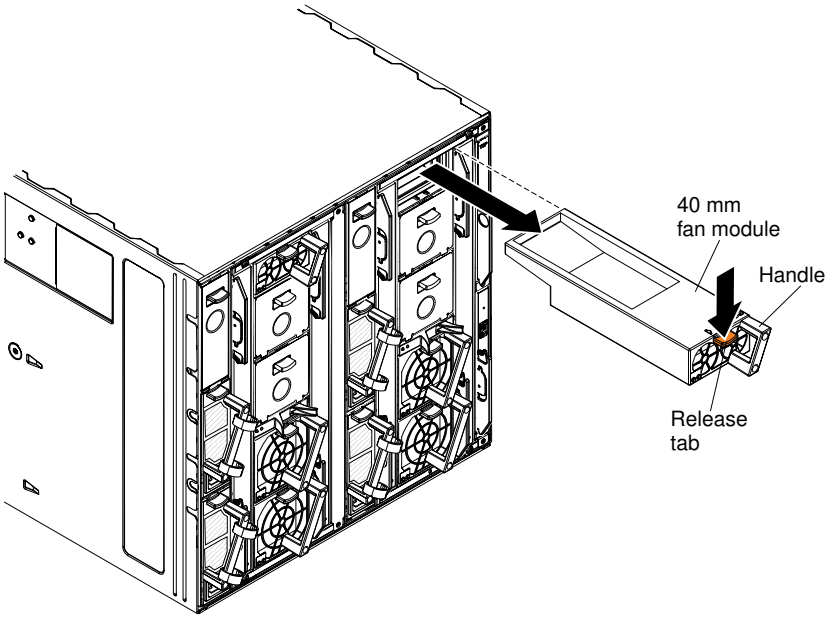
d. Remove the node bay fillers and the chassis shelves, if you want to reduce the weight of the chassis further.See “Removing a chassis shelf” on page 985 for instructions.

Step 2. Remove the components from the rear of the chassis and place them on a flat, static-protective surface.

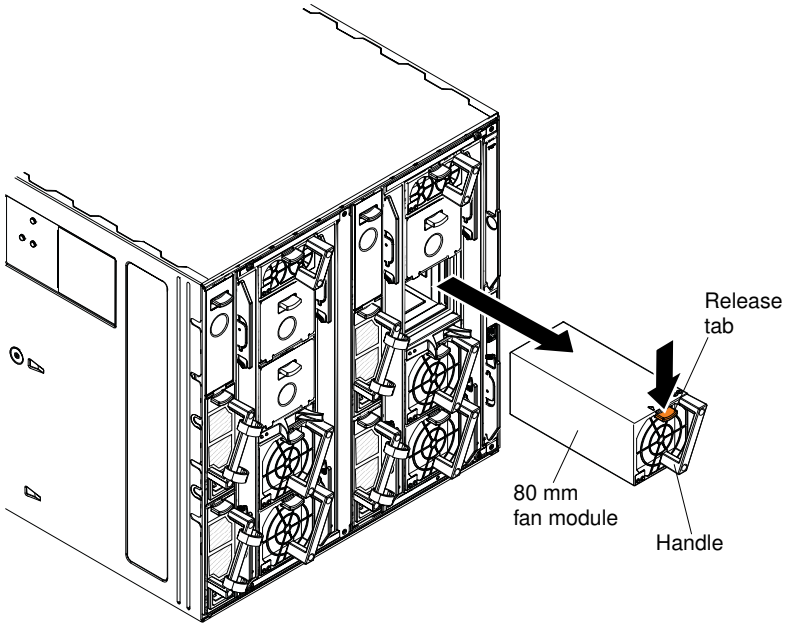
a. Remove all of the power supplies.



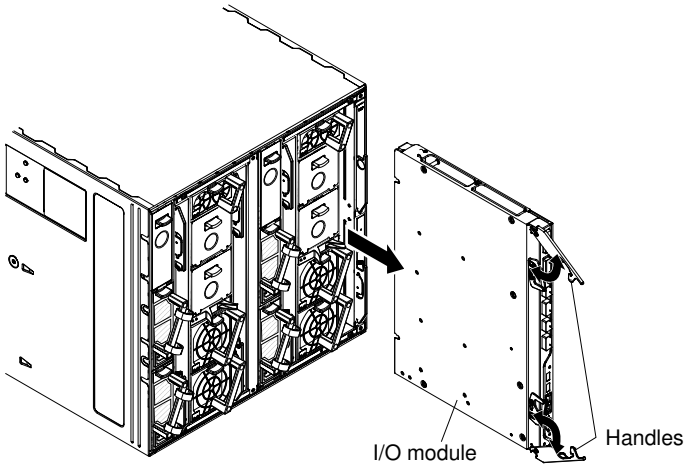
b. Remove both of the 40 mm fan modules.



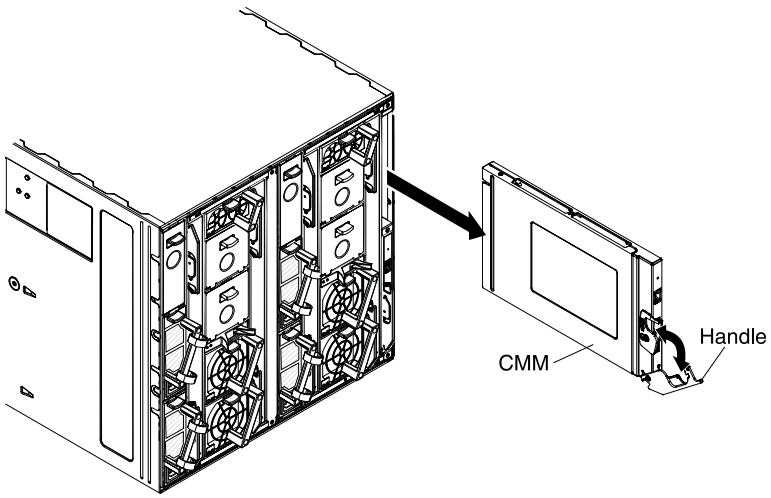
c. Remove all of the 80 mm fan modules.



d. Remove all of the I/O modules.



e. Remove all of the Chassis Management Modules.



Installing the chassis in a rack

Use the information in this section, the rack template, and the rack installation kit that comes with the Flex System Enterprise Chassis to install it in a rack.

Rack Safety Information, Statement 2

DANGER

- **Always lower the leveling pads on the rack cabinet.**
- **Always install stabilizer brackets on the rack cabinet.**
- **Always install servers and optional devices starting from the bottom of the rack cabinet.**
- **Always install the heaviest devices in the bottom of the rack cabinet.**

Before you begin, review the “Installation guidelines” on page 957.

Rack requirements:

- Make sure that the room air temperature is below 40°C (104°F).
- Do not block any air vents; usually, 15 cm (6 in.) of air space in the rear and 5 cm (2 in.) in the front provides proper airflow.
- Three or more people are required to install the device in a rack.
- Do not leave any unused space within a rack open. Fillers must be used to prevent recirculation of warm air.
- Install your Flex System Enterprise Chassis only in a rack that has perforated front and rear doors or in a rack that is equipped with a Rear Door Heat eXchanger.
- Do not extend more than one device out of the rack at the same time.
- Remove the rack doors and side panels to provide easier access during installation.
- The EIA flanges must have holes and clearances per EIA-310-D.
- If you have an adjustable rack, set the distance between the front and rear EIA flanges to 719 mm (28.3 inches) outside to outside.
- Make sure that there is sufficient room in front of the front EIA flange to provide minimum bezel clearance of 50 mm (1.97 inches).
- Make sure that there is sufficient room behind the rear of the rear EIA flanges to provide for cable management and routing.
- Leave 1U of empty space at the top of the rack, if the cables exit at the top, or leave 1U of empty space at the bottom of the rack, if the cables exit at the bottom. This will ensure that the cables don't block service assess to replaceable components.
- Rack weight-handling capacity must be sufficient for the aggregate weight of the populated chassis, power distribution units, and power cables.
- The rack must be stabilized with stabilization brackets and leveling pads so that it does not become unstable when it is fully populated.

To install the chassis in a rack, complete the following steps:

Step 1. Read “Safety” on page iii and “Handling static-sensitive devices” on page 958.

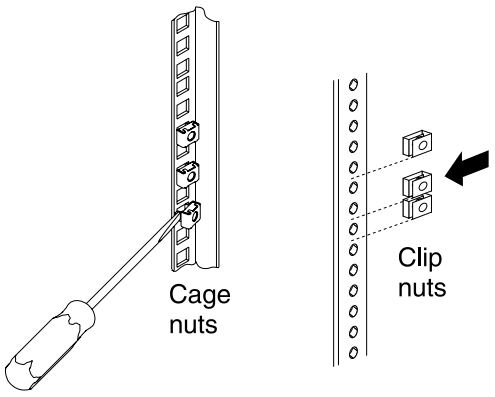
Step 2. Open the rail kit and the rack installation kit that come with the chassis:

- The rail kit box includes the following hardware:
  - One right chassis support rail
  - One left chassis support rail
  - Eight M5x16 combi-head screws (black)
  - Ten strain relief ties
- The rack installation kit includes the following hardware:
  - Twelve M5 cage nuts (use on EIA flanges with square holes)
  - Twelve M5 clip nuts (use on EIA flanges with round holes)
  - Ten M5x16 combi-head screws (black)
  - Eight M5x16 captive washer screws (silver)
  - One right rear support bracket
  - One left rear support bracket
  - One lower rear support bracket

Step 3. If the rack has a door, remove it.

Step 4. Position the rack template that comes with the chassis on the front of the rack at the location where you want to install the chassis. Make sure that the template does not overlap any installed devices, and align the template with the holes in the rack (for an illustration of the template see “Rack template” on page 39). For EIA flanges with square holes, install M5 cage nuts from the rack installation kit in the holes that are indicated on the template.

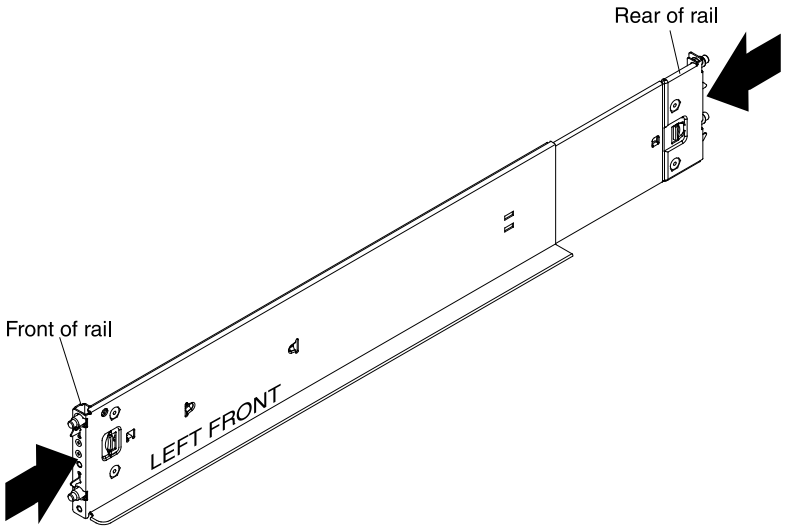
Note: If the EIA flange has round holes, install the M5 clip nuts from the installation kit instead of the M5 cage nuts.



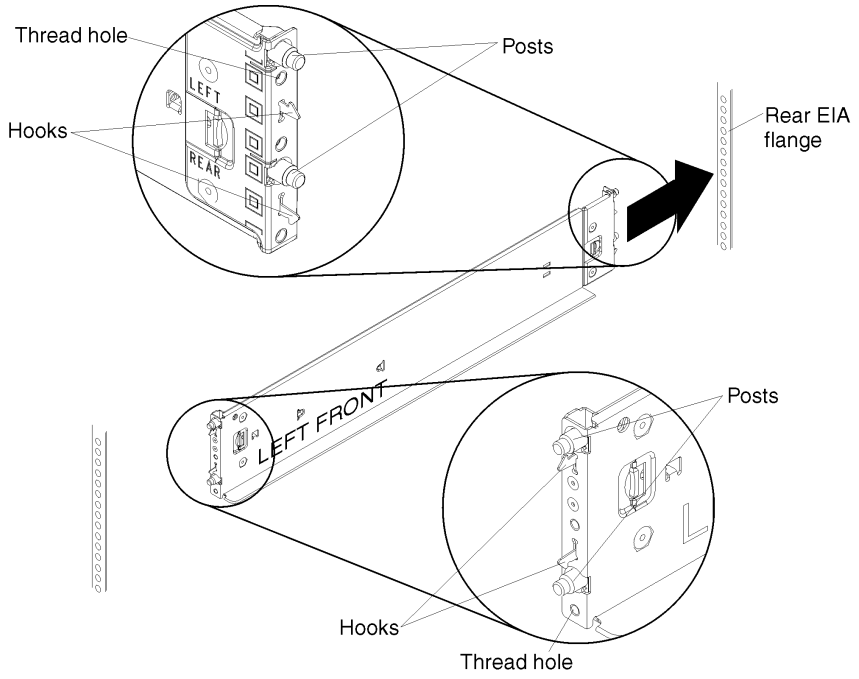
Step 5. Position the rack template on the back of the rack, and install M5 cage nuts in the square holes that are indicated on the template. If the EIA flange has round holes, install the M5 clip nuts from the installation kit.

Note: Make sure that a cage nut or clip nut is installed in every hole indicated on the template.

Step 6. Retract both chassis rails, if they are not already retracted. Rail posts and locking hooks are on each end of each rail.



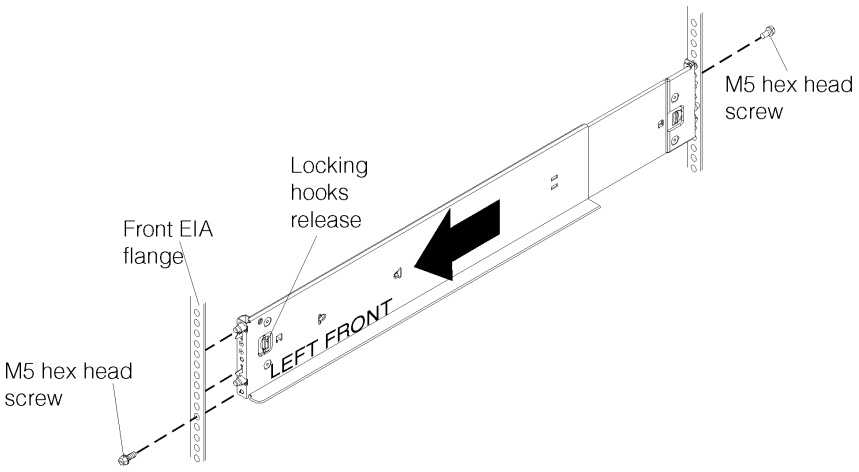
Step 7. Position the left chassis rail in the selected location on the rear of the rack and align the posts on the chassis rail with the holes on the back EIA flange. Insert the posts on the rear of the chassis rail through the holes on the rear EIA flange until the hooks snap into place.



Note:

- Be sure to align the bottom edge of the chassis rail with the bottom U that you want the chassis to rest on.
- If you misalign the chassis rail when you insert it into the holes in the EIA flange, press the locking hooks release on the chassis rail to disengage the hooks and slide the posts out of the holes on the EIA flange. Reinsert the rail into the correct holes on the EIA flange.
- Make sure that the rail posts protrude through the holes on the EIA flanges.

Step 8. Pull the chassis rail forward and insert the posts on the front of the rail into the corresponding holes on the front EIA flange until it snaps into place. Repeat steps 6 through 8 for the right chassis rail.

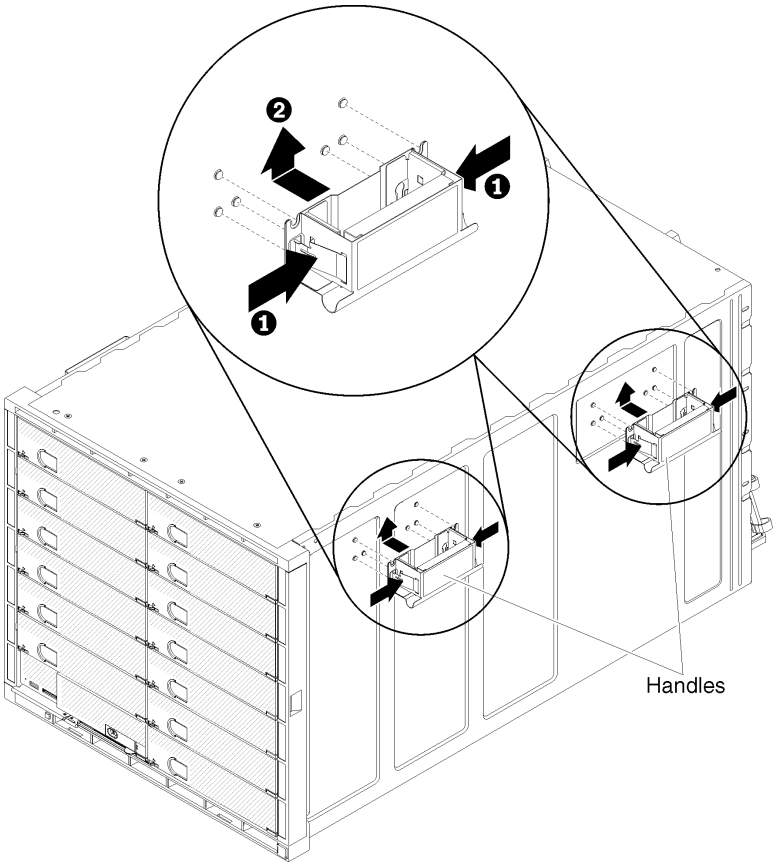


Step 9. Install M5x16 combi-head screws (black) from the rail kit to secure the rails to the EIA flange:

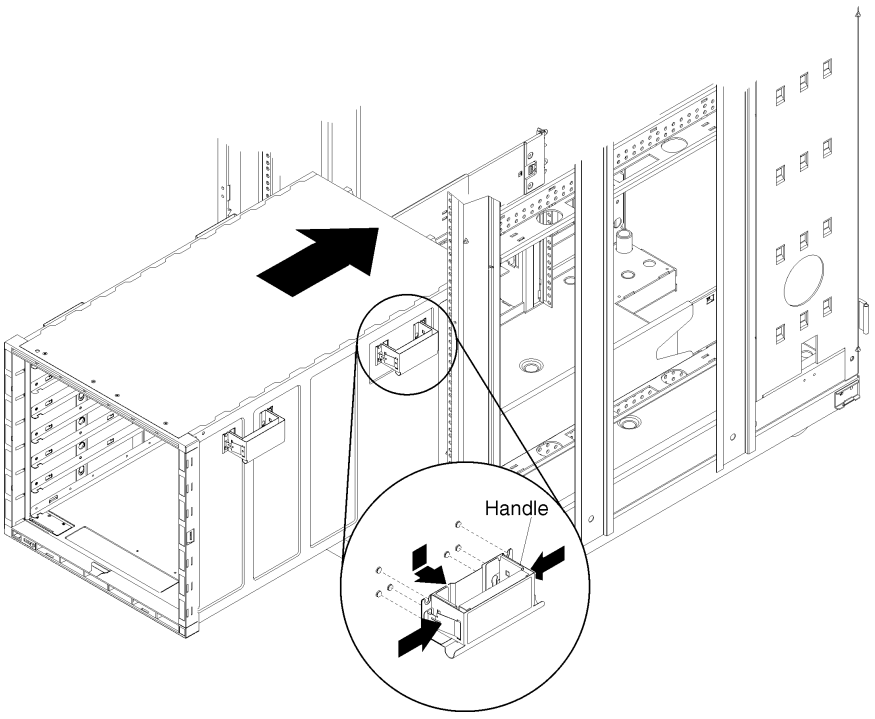
1. At the front of the rack, install an M5x16 combi-head screw (black) in the lower threaded hole on the front of each chassis rail (two screws required, one in the right rail and one in the left rail).
2. At the rear of the rack, install an M5x16 combi-head screw (black) in the upper threaded hole on the rear of each chassis rail (two screws required, one in the right rail and one in the left rail).
3. Tighten the front and rear rail screws to 30 in-lbs (3.4 Nm).

Step 10. Remove the components from the chassis, to make the chassis easier to install in the rack. See "Removing components" on page 27 for instructions. You do not have to remove the two fan logic modules in the rear of the chassis. You can also remove the chassis shelves to further reduce the weight.

Step 11. Attach the chassis handles to the chassis. Four handles come in a box with the chassis. Align the slots on each handle with the posts on the side of the chassis and slide the handle up until it locks into place.

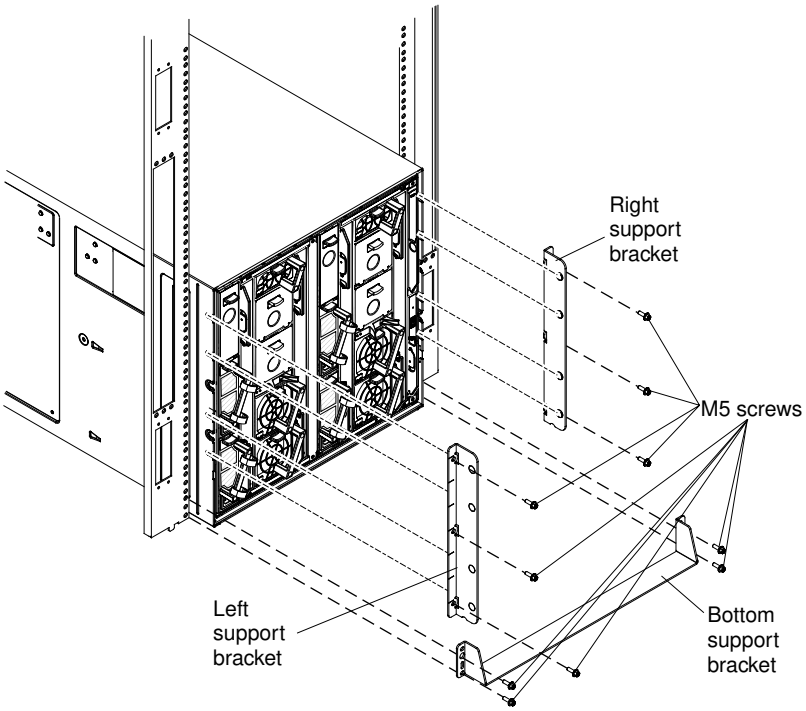


Step 12. Lift the chassis up, place the rear of the chassis onto the chassis rails, and slide the chassis into the rack until the rear chassis handles are near the front EIA flanges. While you support the chassis, remove each rear handle from the chassis (both sides) by pressing inward on the spring-latches on the handle and sliding the handles down to remove them.



Step 13. Slide the chassis farther into the rack until the front chassis handles are near the front EIA flanges, and remove the front handles. Then, slide the chassis all the way into the rack.

Step 14. If you plan to transport the rack to another location with the chassis installed, you must install the rear support brackets.Rear support brackets and mounting screws are provided in the rack installation kit.



a. Facing the rear of the chassis, align the left support bracket with the four slots on the outside of the chassis.

b. Slide the support bracket forward until it locks into place in the slots.

c. Install three M5x16 combi-head screws (black) from the rack installation kit to secure the support bracket to the rack, but do not tighten the screws.

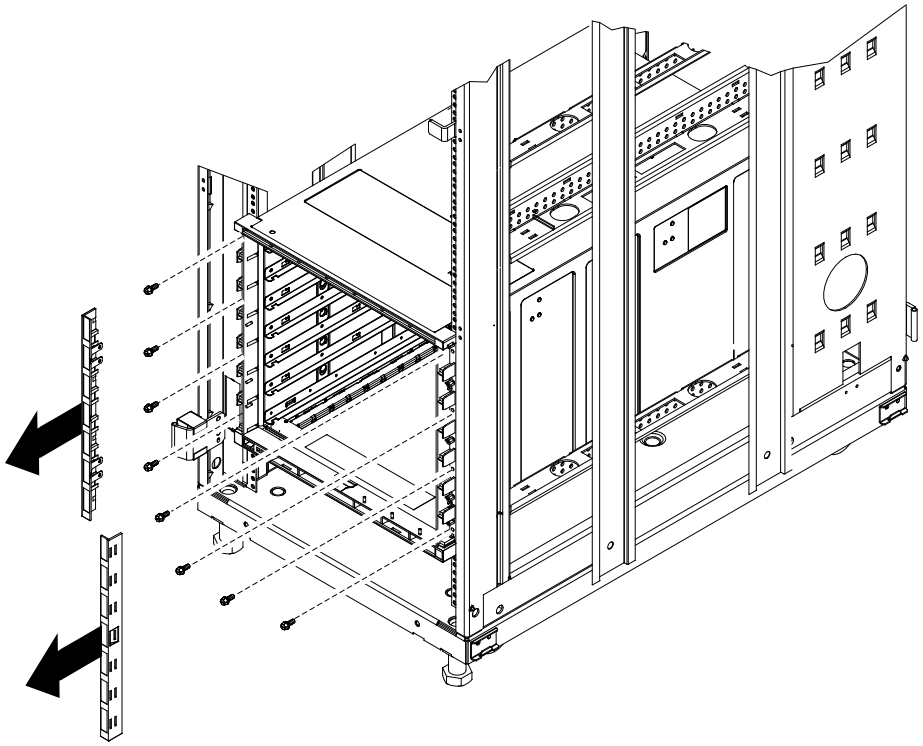
d. Repeat steps 15a through 15c for the right support bracket.

e. Fit the lower support bracket to the bottom of the chassis; then, slide the support bracket forward against the rack.

f. Install four M5x16 combi-head screws (black) from the rack installation kit in the lower support bracket, two screws on the right side and two screws on the left side, but do not tighten the screws.

g. After the right, left, and lower support brackets and screws are installed, tighten all of the screws to 30 in-lbs (3.4 Nm).

Step 15. Remove the plastic label plates from the left and right sides of the chassis.



Step 16. Install eight M5x16 captive washer screws (silver) from the rack installation kit through the front of the chassis (four screws on each side), but do not tighten the screws.

Step 17. After all of the screws are installed, tighten the screws to 30 in-lbs (3.4 Nm).

Step 18. Reinstall the plastic label plates onto the left and right sides of the chassis.

Step 19. Reinstall the chassis shelves, if you removed them earlier.

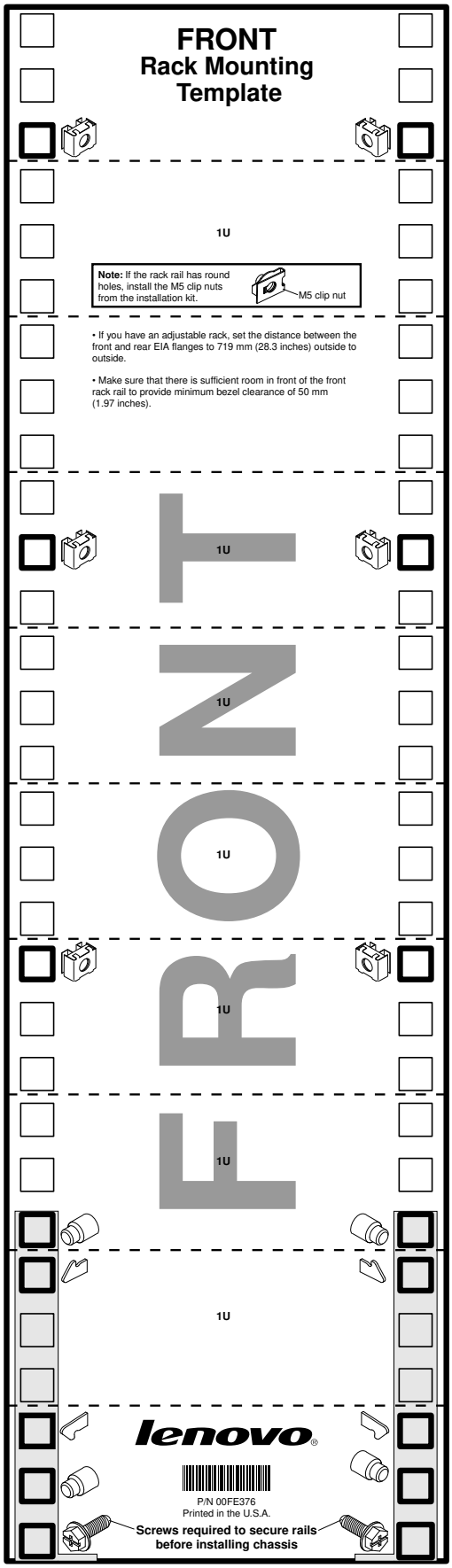
Step 20. Reinstall the components (see “Installing components” on page 41).

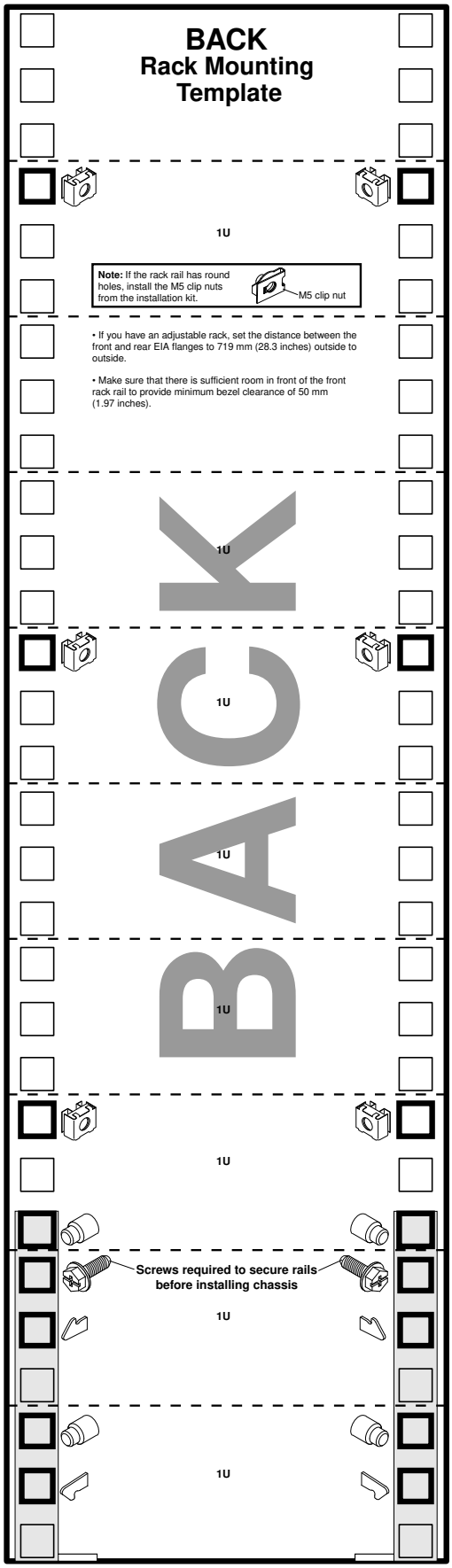
Rack template

The rack template comes with the Flex System Enterprise Chassis.

If you do not have the rack template, you can use the template illustration as a guideline to identify the mounting holes on the front and rear of the rack.

Note: Use this rack template as a guideline only. If you print the template, it might not be printed to scale. You can download a full-size template from http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.8721.doc/printable_doc.html


FRONT
Rack Mounting
Template
1U
Note: If the rack rail has round holes, install the M5 clip nuts from the installation kit.
M5 clip nut
• If you have an adjustable rack, set the distance between the front and rear EIA flanges to 719 mm (28.3 inches) outside to outside.
• Make sure that there is sufficient room in front of the front rack rail to provide minimum bezel clearance of 50 mm (1.97 inches).
FRONT
lenovo
P/N 00FE376
Printed in the U.S.A.
Screws required to secure rails before installing chassis


BACK
Rack Mounting
Template
1U
Note: If the rack rail has round holes, install the M5 clip nuts from the installation kit.
M5 clip nut
• If you have an adjustable rack, set the distance between the front and rear EIA flanges to 719 mm (28.3 inches) outside to outside.
• Make sure that there is sufficient room in front of the front rack rail to provide minimum bezel clearance of 50 mm (1.97 inches).
BACK
Screws required to secure rails before installing chassis

Installing components

After you install the Flex System Enterprise Chassis in a rack, install all of the components in the chassis.

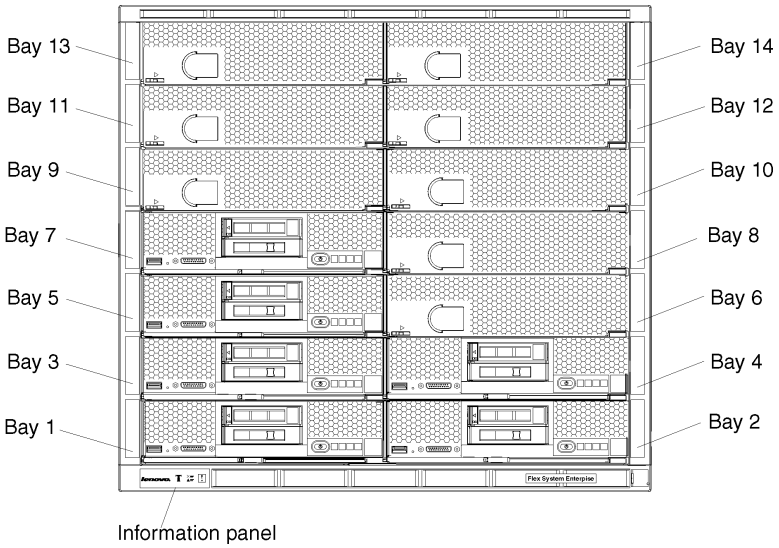
Before you install components in the Flex System Enterprise Chassis:

- Read “Safety” on page iii and “Installation guidelines” on page 957.
- Make sure that the Chassis Management Module firmware is the latest level available. See Updating the CMM firmware"Updating the CMM firmware" in the *Lenovo Flex System Chassis Management Module Installation Guide* for more information.

Important: When you install compute nodes, power supplies, and 80 mm fan modules in the Flex System Enterprise Chassis, install them starting from the bottom up.

Compute nodes

The following illustration shows the locations of node bays in the Flex System Enterprise Chassis.



Note:

A 1-bay compute node occupies one node bay in the chassis.

A 1-bay compute node with captive-mode expansion node occupies two adjacent node bays (horizontally) in the chassis and requires the chassis shelf to be removed prior to installation.

A 2-bay compute node occupies two adjacent node bays (horizontally) in the chassis and requires the chassis shelf to be removed prior to installation.

A 4-bay storage node or storage expansion enclosure occupies four adjacent node bays (two vertically and horizontally) in the chassis and requires the chassis shelves and shelf supports to be removed prior to installation.

Power supplies

The chassis power load is dependent on the number and type of compute nodes, storage nodes, I/O modules, and management modules that are installed in the chassis. The number and type of power supplies that you install determines how much power is available to power all of these devices. The amount of power available must be sufficient for the expected chassis load.

You can use the Lenovo Capacity Planner to determine the power load for a specific chassis configuration. See https://datacentersupport.lenovo.com/tw/en/products/solutions-and-software/software/lenovo-capacity-planner/solutions/ht504651 for more information.

Important:

- Up to six power supplies can be installed.
- Do not mix different types of power supplies in the Flex System Enterprise Chassis.
- Each chassis must contain either all ac-powered supplies or all dc-powered supplies.
- For ac-powered chassis, do not mix 2100 W and 2500 W power supplies. Chassis powered by ac power should contain only power supplies of the same wattage.
- Install power supplies from the bottom up starting with power bays 1 and 4, then power bays 2 and 5, then power bays 3 and 6.

Install power supplies according to the number of populated node bays as shown in Table 6 “Required power supplies relative to the number of populated node bays” on page 42. See also “Power supplies” on page 20 for more information.

Table 6. Required power supplies relative to the number of populated node bays

Number of populated node bays	Power supplies required
1 - 4	2
5 - 6	3
7 - 8	4
9 - 11	5
12 - 14	6

80 mm fan modules

The number and type of 80 mm fans that you install depends on the type of power supplies that are installed in the chassis and the number of populated node bays. Up to eight 80 mm fan modules can be installed.

Important:

- Chassis with 2100 W power supplies must have 80 mm single-fan modules.
- Chassis with 2500 W power supplies must have 80 mm dual-fan modules.
- Use only the same type of 80 mm fan module in each chassis. Do not mix single-fan and dual-fan 80 mm fan modules within a chassis.

Install 80 mm fan modules according to the number of populated node bays as shown in Table 7 “Required 80 mm fan modules relative to the number of populated node bays” on page 42. See also “Fan modules” on page 22 for more information.

Table 7. Required 80 mm fan modules relative to the number of populated node bays

Fan zone 1 (behind node bays 1, 3, 5, 7, 9, 11, and 13)		Fan zone 2 (behind node bays 2, 4, 6, 8, 10, 12, and 14)	
Number of populated node bays	**80 mm fans required**	**Number of populated node bays**	**80 mm fans required**
1 - 2	2	1 - 2	2
3 - 4	3	3 - 4	3
5 - 7	4	5 - 7	4

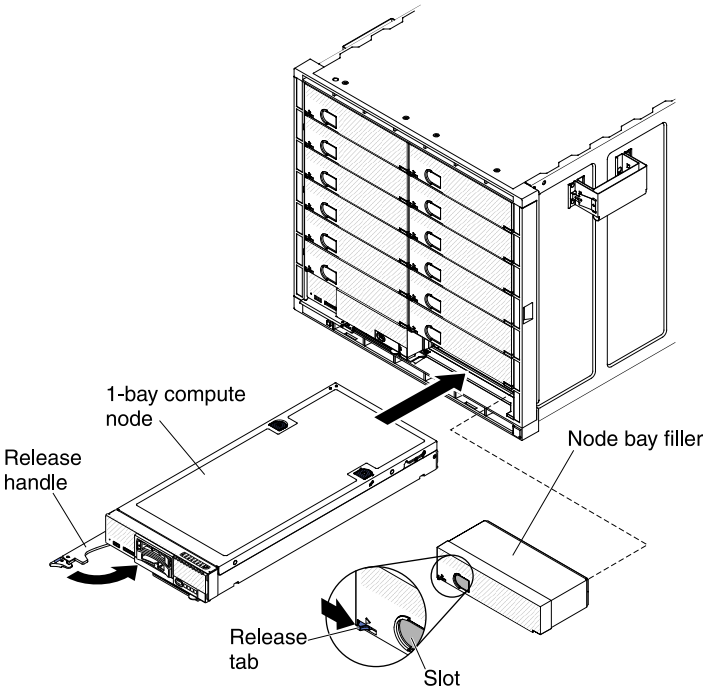
Installing a 1-bay compute node

You can install up to fourteen 1-bay compute nodes in the Flex System Enterprise Chassis. Compute nodes are installed in the front of the Flex System Enterprise Chassis.

Before you install a compute node in the Flex System Enterprise Chassis, complete the following steps:

1. Verify that the compute node is compatible with the chassis. See http://www.lenovo.com/serverproven/.
2. Make sure that enough power supplies and fan modules are installed in the chassis to support the compute node. See “Installing components” on page 41 to determine the number of power supplies and 80 mm fan modules that are required and where they should be installed in your chassis configuration.
3. Read the instructions that come with the compute node.
4. Make sure that you have installed any optional hardware devices in the compute node.
5. Select the bay for the compute node.

To install a 1-bay compute node, complete the following steps.



Step 1. Remove the node bay filler, if one is installed. Push the filler release tab to the right; then, grasp the filler by the slot and pull it out of the bay.

Step 2. Open the release handle (rotate the handle to the left).

Step 3. Slide the compute node into the node bay until it is seated.

Step 4. Close the release handle (rotate the handle to the right).

After you install the compute node, make a note of the compute node identification information on one of the labels that come with the Flex System Enterprise Chassis. Place a label on the node label tab and on the adjacent chassis label plate, to the right or left of the compute node (depending on the bay in which the compute node is installed). See “User labels” on page 59 for more information.

Important: Do not place the label on the compute node or in any way block the ventilation holes on the chassis.

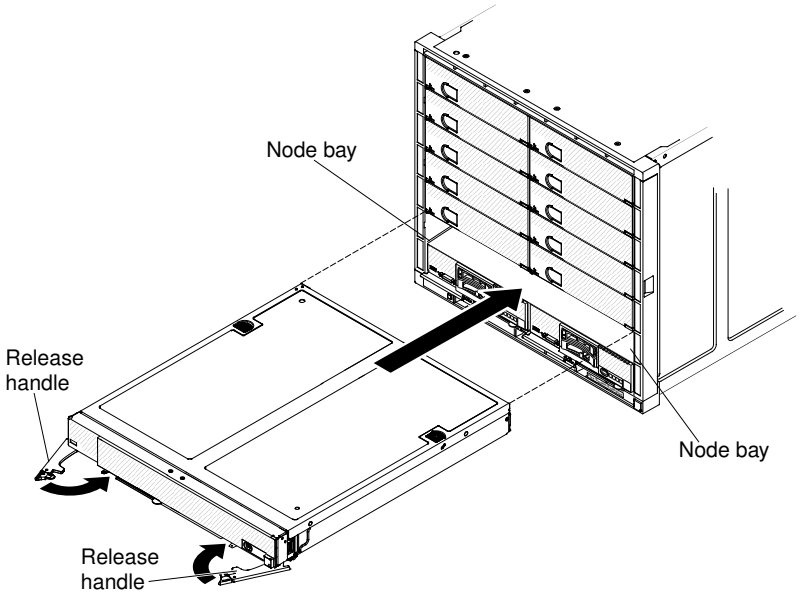
Installing a 2-bay compute node

You can install up to seven 2-bay compute nodes in the chassis. A 2-bay device occupies two adjacent node bays (horizontally) in the chassis.

Before you install a compute node in the Flex System Enterprise Chassis, complete the following steps:

1. Verify that the compute node is compatible with the chassis. See http://www.lenovo.com/serverproven/.
2. Make sure that enough power supplies and fan modules are installed in the chassis to support the compute node. See “Installing components” on page 41 to determine the number of power supplies and 80 mm fan modules that are required and where they should be installed in your chassis configuration.
3. Read the instructions that come with the compute node.
4. Make sure that you have installed any optional hardware devices in the compute node.
5. Select the bays for the compute node. Two adjacent bays are required.
6. Remove the fillers and the chassis shelf from the selected bays, if they are installed. See “Removing a chassis shelf” on page 985 for instructions.

To install a 2-bay compute node, complete the following steps.



Step 1. Open both release handles (rotate the left handle to the left and rotate the right handle to the right).

Step 2. Slide the compute node into the node bays until it is seated.

Step 3. Close both release handles.

After you install the compute node, make a note of the compute node identification information on one of the labels that come with the Flex System Enterprise Chassis. Place a label on the node label tab and on the adjacent chassis label plate, to the left of the compute node. See “User labels” on page 59 for more information.

Important: Do not place the label on the compute node or in any way block the ventilation holes on the chassis.

Installing a 4-bay storage enclosure

A 4-bay storage enclosure occupies four adjacent node bays in the chassis.

A storage system includes a control enclosure and might also include one or more expansion enclosures. Refer to the documentation that comes with the storage enclosure for detailed information about installing, cabling, and configuring the storage enclosure. Storage node documentation is available from http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.4939.doc/site_product_page.html.

Before you install a 4-bay storage enclosure in the Flex System Enterprise Chassis, complete the following steps:

1. Verify that the storage enclosure is compatible with the chassis. See http://www.lenovo.com/serverproven/.
2. Make sure that enough power supplies and fan modules are installed in the chassis to support the storage enclosure and any expansion enclosures that you plan to install. See “Installing components” on page 41 to determine the number of power supplies and 80 mm fan modules that are required and where they should be installed in your chassis configuration.
3. Select the bays for the storage enclosure. Four adjacent bays (two vertically and horizontally) are required.
4. Remove the node fillers and the chassis shelves from the selected bays, if they are installed. See “Removing a chassis shelf” on page 985 for instructions.
5. Remove the shelf supports from the center of the selected bays, if they are installed. See “Removing the shelf supports” on page 960 for instructions.

Complete the following steps:

Step 1. Follow the detailed instructions that come with the 4-bay storage enclosure to install, cable, and configure the storage enclosure.Storage node documentation is available from http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.4939.doc/site_product_page.html.

After you install the storage enclosure, complete the following steps:

1. Make a note of the enclosure identification information on one of the labels that come with the Flex System Enterprise Chassis. Place a label on the enclosure label tab and on the adjacent chassis label plate, to the left of the storage enclosure. See “User labels” on page 59 for more information.

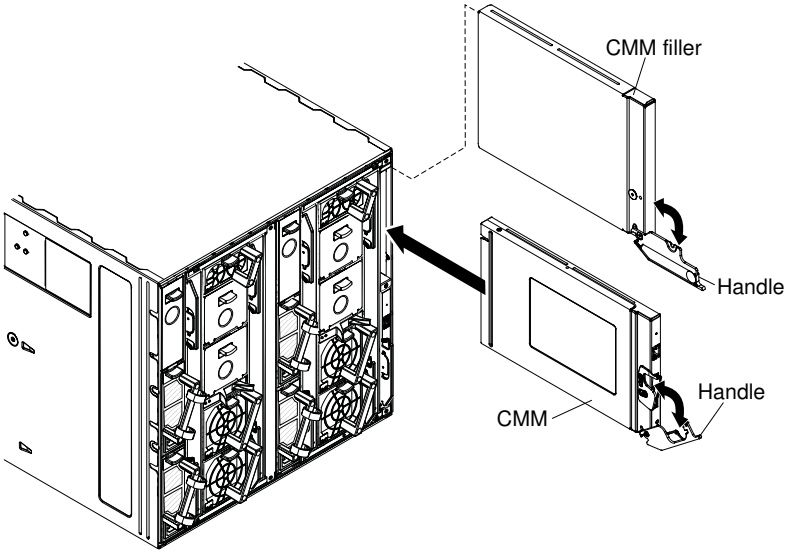
   Important: Do not place the label on the storage enclosure or in any way block the ventilation holes on the chassis.

Installing a Chassis Management Module

You can install up to two Chassis Management Modules for redundancy support in the Flex System Enterprise Chassis.

Before you install the Chassis Management Module, read the installation instructions that come with the Chassis Management Module (see http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.cmm.doc/cmm_product_page.html).

To install a Chassis Management Module (CMM), complete the following steps.



Step 1. If a filler is installed in the CMM bay, remove it. Rotate the release handle on the filler down and slide it out of the bay.

Step 2. Press the CMM release latch down and rotate the CMM handle down until it stops.

Step 3. Align the CMM with the bay and slide it into the bay until it is seated.

Step 4. Close the handle (rotate the handle up) so that it locks in place.

Note: Make sure that the power-on LED on the CMM is lit. This indicates that the CMM is operating correctly. See "CMM controls and indicators" on page 17 to locate the LED.

When you install a CMM, if the chassis is not connected to a DHCP server on the network, it takes up to 3 minutes for the CMM to use the default (static) IP address.

After failover, you might have to wait as long as 5 minutes to establish a network connection to the CMM. Some networks include switches, routers, and hubs that do not allow (or relay) an address resolution protocol (ARP) from the new CMM to update the network cached ARP table. Without this information relay, the new MAC address/IP association will not recognize the CMM. 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 CMM.

After you install the Chassis Management Module, complete the following steps:

1. Connect all cables to the CMM.
2. Configure the CMM, by loading a previously saved configuration or by going through the Flex System Manager management software configuration wizard.

Installing a Flex System Manager management node

You can install one Flex System Manager management node in a multiple-chassis configuration. You can install up to two Flex System Manager management nodes in a multiple-chassis configuration for redundancy. One management node can be installed in two of the chassis in a multiple-chassis configuration.

Before you install the Flex System Manager management node, complete the following steps:

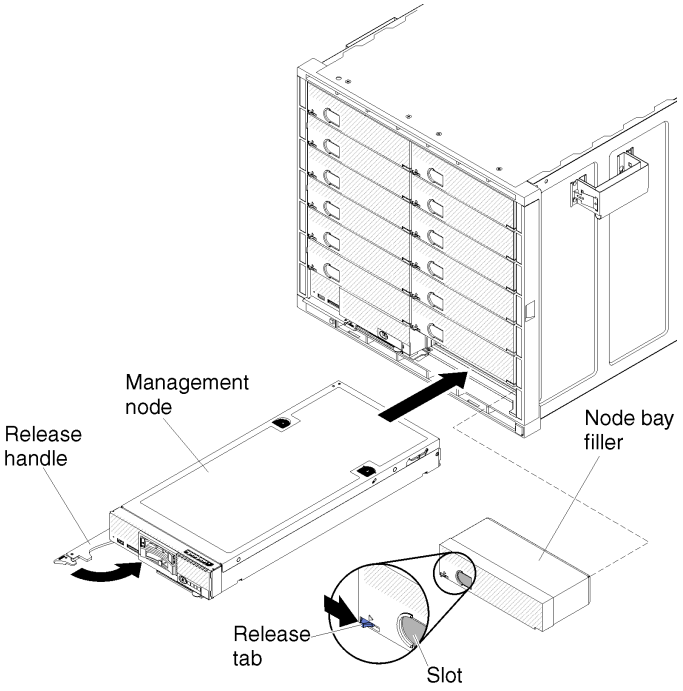
1. Make sure that enough power supplies and fan modules are installed in the chassis to support the management node. See "Installing components" on page 41 to determine the number of power supplies and 80 mm fan modules that are required and where they should be installed in your chassis configuration.

2. Read the Flex System Manager management node hardware description (see the *Flex System Manager Installation and Service Guide* for more information).
3. Select the bay for the management node.

Attention:

- If you are installing two management nodes in separate chassis of a multiple-chassis configuration, they must *not* be installed in the same node bay. For example, if you install the first management node in node bay 1 in one of the chassis, install the second management node in a *different* chassis in any node bay other than node bay 1.
- The management nodes default static IP address depends in part on the node bay that it is installed in. If you install two management nodes in the same node bay in different chassis in a multiple-chassis configuration, they will have the same default IP address.

To install a Flex System Manager management node, complete the following steps.



Step 1. Remove the bay filler, if one is installed. Push the filler release tab to the right; then, grasp the filler by the slot and pull it out of the bay.

Step 2. Open the release handle (rotate the handle to the left).

Step 3. Slide the management node into the chassis bay until it is seated.

Step 4. Close the release handle (rotate the handle to the right).

After you install the Flex System Manager management node, complete the following steps:

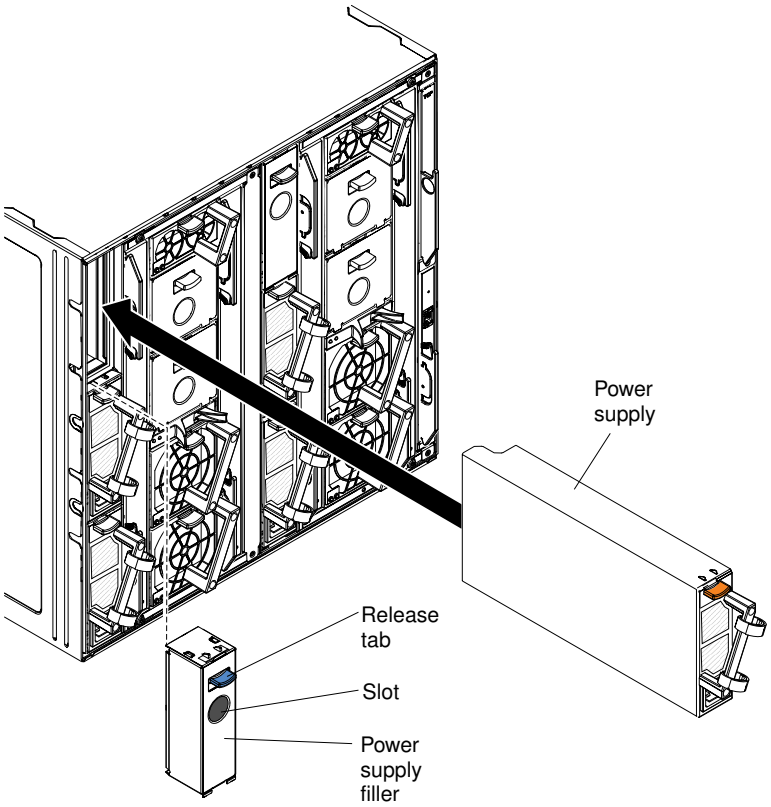
1. Connect all cables to the management node.
2. Configure the management node (see http://flexsystem.lenovofiles.com/help/index.jsp for more information).

Installing a power supply

The Flex System Enterprise Chassis comes with two power supplies already installed in the rear of the chassis. You can install up to four additional power supplies in the chassis for a total of six power supplies.

Note: The number of power supplies that you install is dependent on the type of power supply, the chassis power load, and selected chassis power policy.

To install a power supply, complete the following steps.

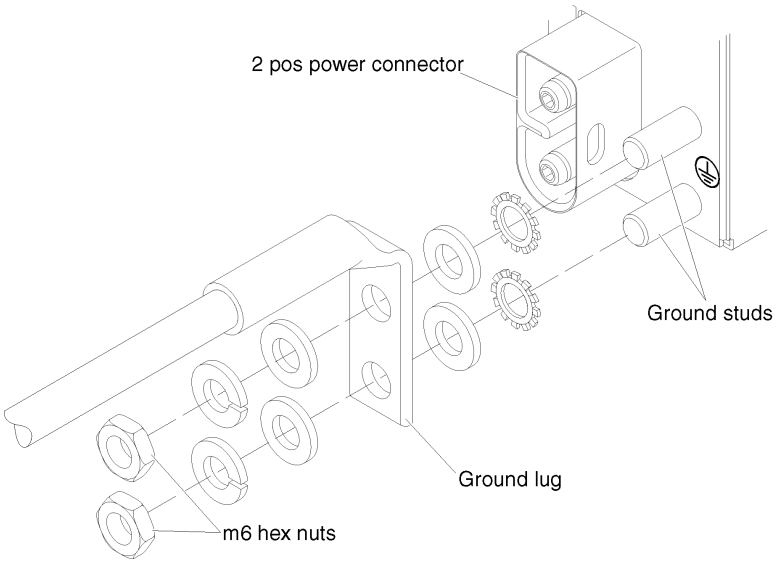


Step 1. If you are adding a power supply, remove the filler from the power-supply bay in which you want to install the power supply (press the release tab, grasp the filler by the slot, and pull it out of the bay).

Step 2. Grasp the power-supply handle and slide the power supply into the bay until it locks in place.

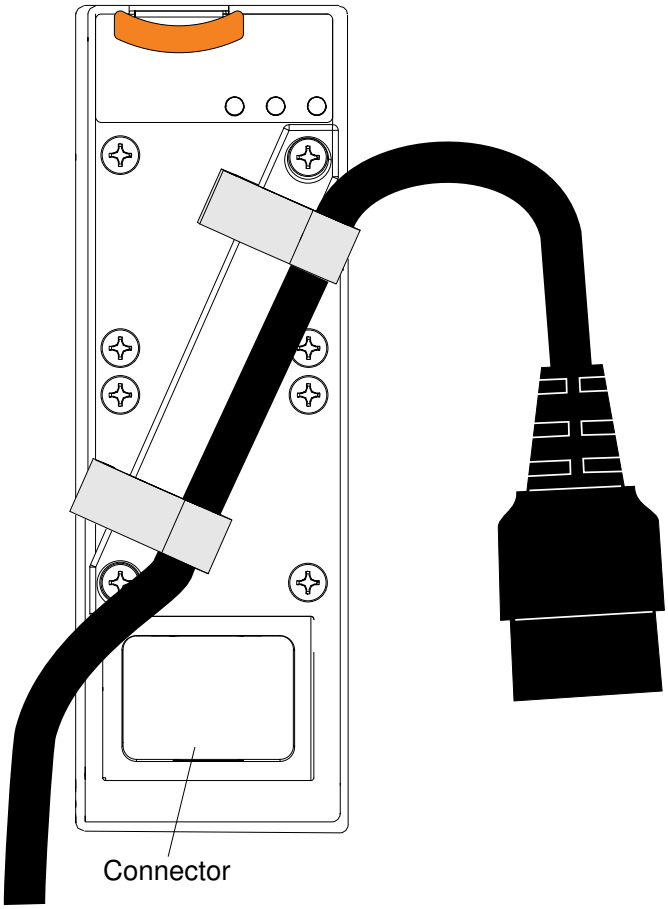
Step 3. If you are installing a -48 to -60 V dc power supply, connect the earth ground cable to the power supply.

1. Use a 10 mm nut driver to remove the hex nuts from the ground studs.
2. Remove the lock washer and one of the flat washers from each ground stud.
3. Push the ground lug onto the ground studs; then, place the flat washer, the lock washer, and the hex nut back on each ground stud.
4. Use a 10 mm nut driver to tighten the hex nuts to 4.0 - 4.8 Newton-meters (35.4 - 42.5 inch-pounds).

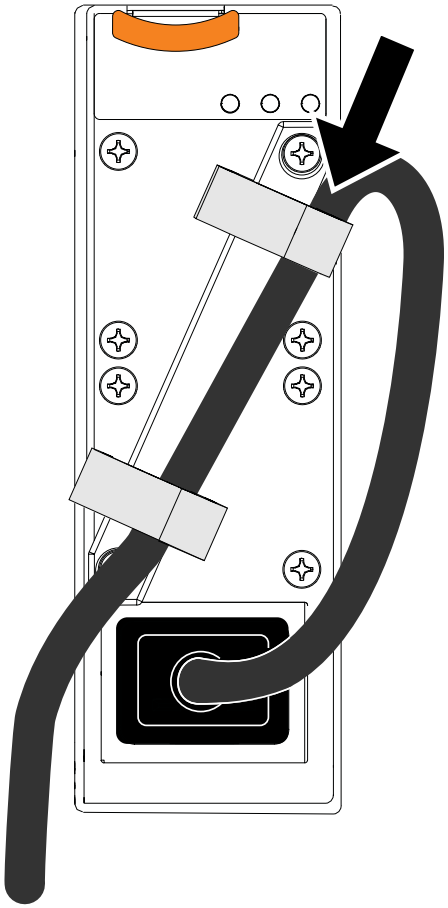


Step 4. Connect the power cord to the power supply:

1. Loosen the strain-relief ties that are attached to the power-supply handle, but do not remove them.
2. Align the power cord with the power-supply handle; then, secure the cord to the handle with the strain-relief ties.



3. Loop the power cord connector around and connect it to the power supply.



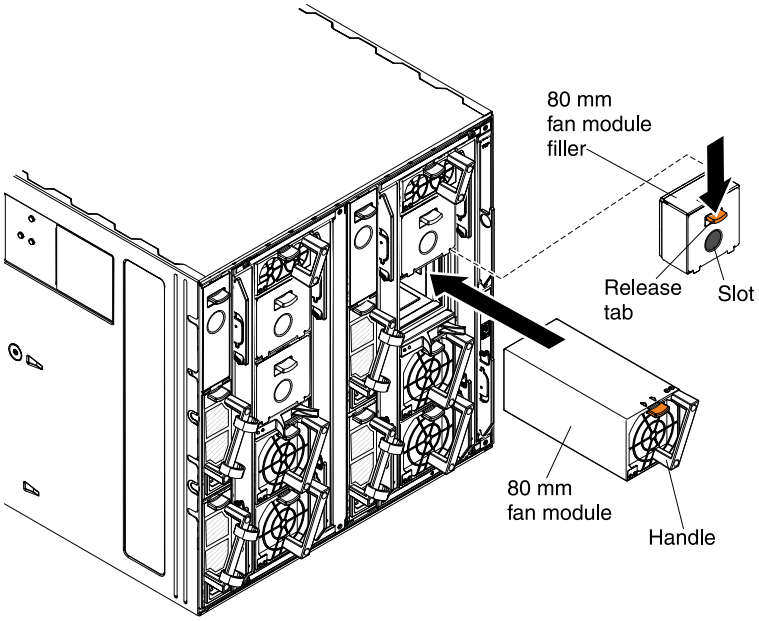
4. Push the power cord back through the strain-relief ties to remove excess cable from the loop.

Installing a 80 mm fan

The Flex System Enterprise Chassis comes with four 80 mm fan modules already installed in the rear of the chassis. You can install up to four additional 80 mm fan modules for a total of eight 80 mm fan modules.

See “Installing components” on page 41 to determine the number of 80 mm fan modules that are required and where they should be installed in your chassis configuration.

To install a 80 mm fan module, complete the following steps.



.

Step 1. Remove the fan module filler, if one is installed.

Step 2. Grasp the fan module by the handle and align it with the fan bay.

Step 3. Slide the fan module into the chassis until it locks in place.

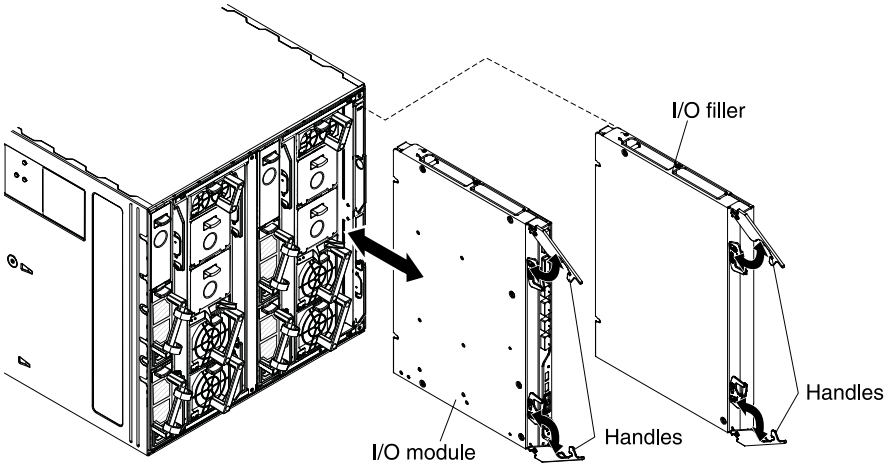
Installing an I/O module

You can install up to four I/O modules into the Flex System Enterprise Chassis. An Ethernet switch or a pass-thru module must be installed in I/O bay 1 and/or bay 2 whenever one or more compute nodes on-board Ethernet interface is active or there is an Ethernet I/O expansion card interfacing with I/O bay 1 and 2.

Before installing an I/O module, complete the following steps:

1. Verify that the I/O module is compatible with the chassis. See http://www.lenovo.com/serverproven/.
2. Read the installation instructions that come with the I/O module.

To install an I/O module, complete the following steps.



Step 1. Remove the I/O filler, if necessary. Open the release handles (rotate the top handle up and the bottom handle down).

Step 2. Slide the filler out of the bay.

Step 3. Open the release handles on the I/O module (rotate the top handle up and the bottom handle down).

Step 4. Align the I/O module with the bay on the chassis and slide the module into the module bay until it is seated.

Step 5. Close the release handles (rotate the top handle down and bottom handle up).

Network integration with the Flex System Manager

In Flex System Enterprise Chassis with the Flex System Manager management node, you have the option to configure separate management and data networks.

The network configuration is established by the Flex System Manager management software during initial setup. You can also change the network configuration after initial setup by clicking the **Administration** tab in the Flex System Manager user interface.

You can use Flex System Manager management software to configure the network attributes for each network. Configuration parameters such as IPv4 or IPv6 address, subnet mask (IPv4), domain name servers, gateways, DHCP, and customized network routing information for each network are supported.

Important: When you establish two separate networks, establish network routing entries that define which network should be used for various network segments within the larger network.

Note:

- The illustrations in this section show management and data network examples when a single Chassis Management Module is installed in the chassis. Dual CMMs provide redundancy for the management fabric within the chassis as well as two separate uplinks from the chassis to the external network devices. You may choose to connect the redundant CMMs to redundant external Ethernet fabrics for added fault protection. The redundant CMMs within a chassis will automatically select the correct mode of operation based upon chassis and network status.
- Due to the design of the Flex System Enterprise Chassis, it is important to have all management network traffic on a separate subnet than the data traffic. This means all CMMs, IMMs, FSPs, and switch management interfaces should be on a different subnet/VLAN than the data production traffic of the other chassis components (such as node operating systems).

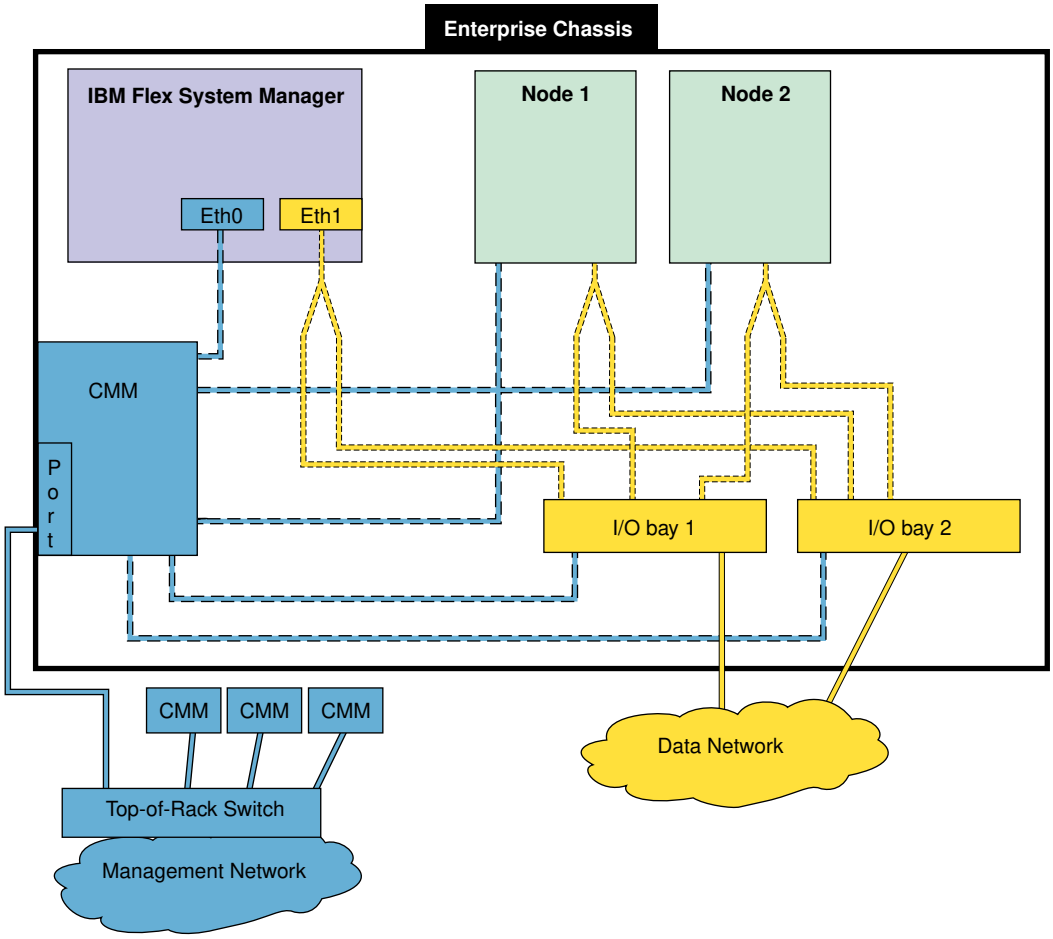
Management network

The Flex System Manager management node has two Ethernet interfaces which can be configured. The Eth0 port is connected to the Chassis Management Module (CMM) external Ethernet port through the chassis internal management network, effectively extending the chassis management network outside of the chassis. The CMM is connected to a top-of-rack switch that provides a central connection point for all chassis hardware to be managed by the Flex System Manager management software. These connections are referred to as the *management network*.

The management network is used to complete management-related functions for the various endpoints that are managed by the Flex System Manager management software, such as other Flex System Enterprise Chassis and compute nodes. During initialization the management software discovers any Flex System Enterprise Chassis on the management network. Note that the management node console can be connected to the management network or to the data network.

Note: If you want to configure your network so that the entire network is set up on a single IP subnet, configure just Eth0 on the Flex System Manager management node. If you choose to configure Eth0 and Eth1, you must configure them on different IP subnets.

Example of Separate Management and Data Networks



Data network

The Flex System Manager management node Eth1 port must be connected to the chassis switch modules that are installed in I/O bay 1 or bay 2. This is referred to as the *data network*. You can configure a switch module in bay 1 or bay 2 to map Eth1 to one of its external Ethernet ports, as you would configure the other nodes in the chassis that are connected to the external network. The data network is used by applications and operating systems and can support data transfer rates up to 10 Gbps if a chassis switch module that is capable of 10 Gbps is installed.

One of the key functions that the data network supports is discovery of operating systems on the various network endpoints. Discovery of operating systems by the Flex System Manager is required to support software updates on an endpoint such as a compute node. The Flex System Manager Checking and Updating Compute Nodes wizard assists you in discovering operating systems as part of the initial setup.

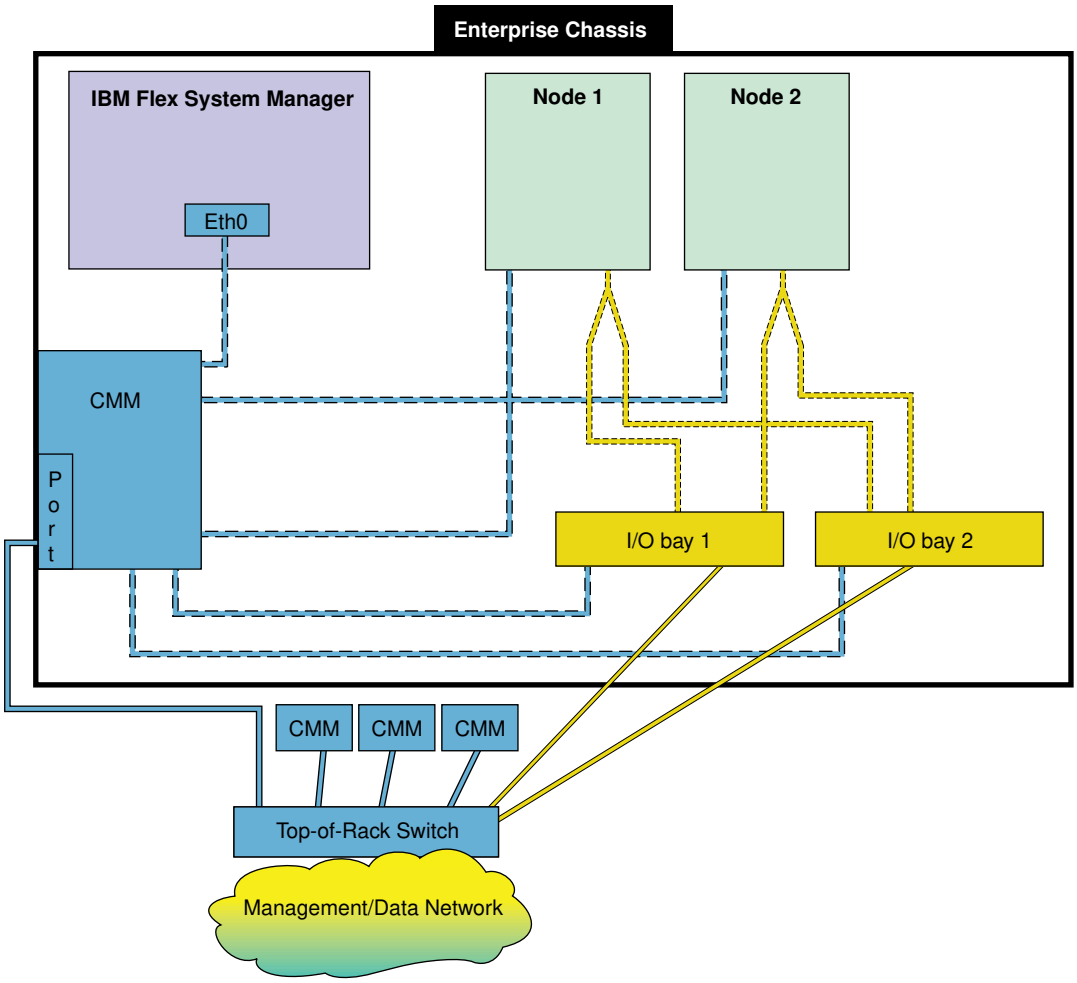
When you set up a high-availability environment that consists of active and passive Flex System Manager management nodes, either the management network or the data network can be used to replicate the data from the active management node to the passive management node. The additional bandwidth that is supported on the data network can improve data replication performance between active and passive management nodes.

Single network configuration

You can also set up your environment so that the management network and data network are the same network. This is typically a simpler approach to network configuration and results in an easier setup process. Typically, a single gateway can be used, and network routing table configuration can use default values that are established by the Flex System Manager setup wizard.

Note: When you are using a single network configuration, users and applications that have access to the data network also have access to the management network.If separating data and management access is important for security considerations, you should use separate data and management networks.

Example of Single Management and Data Network



Cabling the chassis

Cabling the Flex System Enterprise Chassis requires a site integration plan that describes the network environment. Make sure that you have completed all planning activities before you connect the network cables.

Cabling to the network components in the Flex System Enterprise Chassis will vary depending on the number of chassis, the type of I/O modules and management devices that you have purchased, and the planned network environment. See the site integration plan for more information about cabling the network.

Planning information is available from http://flexsystem.lenovofiles.com/help/index.jsp.

Information about cabling network switches is available from http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.networkdevices.doc/network_iomodule.html.

See “Connecting the chassis to power” on page 55 for information about connecting the chassis power cords.

Connecting the chassis to power

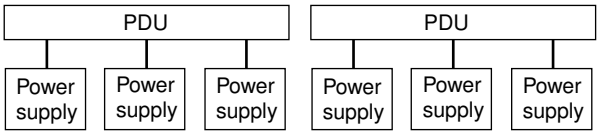
Power is supplied to the Flex System Enterprise Chassis when one end of each power cord is connected to a power connector on the rear of the chassis and the other end of each power cord is connected to a power distribution unit (PDU) or uninterruptible power source (UPS).

Connecting for N+N power redundancy

The Flex System Enterprise Chassis can have up to six power supplies. The chassis allows you to populate power supplies to meet the load demand that is installed in the chassis. As more nodes are installed in the chassis, you can install additional power supplies to meet the increased load demand.

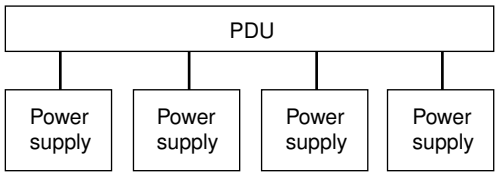
Attention: If there is not enough power available from the power supplies to meet the load demand installed in the chassis, the Chassis Management Module will not allow some of the devices to power on.

To provide power source redundancy for the chassis, you can connect the power supplies in an N+N configuration, where N can be 1, 2 , or 3, depending on the total load installed in the chassis. In this configuration, the power-supply power cords are connected to separate PDUs. If a supply circuit fails, the remaining power supplies have enough power available to power the entire chassis load. A fully configured chassis with N+N power redundancy has six power supplies.



Connecting for N+1 power redundancy

If power source redundancy is not a concern but you want power supply redundancy, you can connect the power supplies in an N+1 configuration, where N can be 1, 2, 3, 4, or 5 depending on the total load that is installed in the chassis. In this configuration, the power-supply power cords are connected to the same PDU but there is one extra power supply available (+1). If one of the power supplies fails, the remaining power supplies have enough power available to power the entire chassis load. If two or more power supplies fail, it is possible for the entire chassis to lose power. If the power source circuit fails, the entire chassis will lose power.



Note: The Flex System Enterprise Chassis does not have a power switch. See “Disconnecting the chassis from power” on page 60 for more information.

Statement 29

CAUTION:
This equipment is designed to permit the connection of the earthed conductor of the dc supply circuit to the earthing conductor at the equipment. If this connection is made, all of the following conditions must be met:

- **This equipment shall be connected directly to the dc supply system earthing electrode conductor or to a bonding jumper from an earthing terminal bar or bus to which the dc supply system earthing electrode conductor is connected.**
- **This equipment shall be located in the same immediate area (such as, adjacent cabinets) as any other equipment that has a connection between the earthed conductor of the same dc supply circuit and the earthing conductor, and also the point of earthing of the dc system. The dc system shall not be earthed elsewhere.**
- **The dc supply source shall be located within the same premises as this equipment.**
- **Switching or disconnecting devices shall not be in the earthed circuit conductor between the dc source and the point of connection of the earthing electrode conductor.**

Statement 31

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 power source.**
- **Connect to properly wired power sources 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 ac power cords, dc power sources, network connections, telecommunications systems, and serial cables before you open the device covers, unless you are instructed otherwise in the installation and configuration procedures.**
- **Connect and disconnect cables as described in the following table when you install, move, or open covers on this product or attached devices.**

To Connect:

1. Turn OFF all power sources and equipment that is to be attached to this product.
2. Attach signal cables to the product.
3. Attach power cords to the product.
   - For ac systems, use appliance inlets.
   - For dc systems, ensure correct polarity of -48 V dc connections: RTN is + and -48 V dc is -. Earth ground should use a two-hole lug for safety.
4. Attach signal cables to other devices.
5. Connect power cords to their sources.
6. Turn ON all the power sources.

To Disconnect:

1. Turn OFF all power sources and equipment that is to be attached to this product.
   - For ac systems, remove all power cords from the chassis power receptacles or interrupt power at the ac power distribution unit.
   - For dc systems, disconnect dc power sources at the breaker panel or by turning off the power source. Then, remove the dc cables.
2. Remove the signal cables from the connectors.
3. Remove all cables from the devices.

Statement 34

CAUTION:
To reduce the risk of electric shock or energy hazards:

- **This equipment must be installed by trained service personnel in a restricted-access location, as defined by the NEC and IEC 60950-1, First Edition, The Standard for Safety of Information Technology Equipment.**
- **Connect the equipment to a properly grounded safety extra low voltage (SELV) source. A SELV source is a secondary circuit that is designed so that normal and single fault conditions do not cause the voltages to exceed a safe level (60 V direct current).**
- **Incorporate a readily available approved and rated disconnect device in the field wiring.**
- **See the specifications in the product documentation for the required circuit-breaker rating for branch circuit overcurrent protection.**
- **Use copper wire conductors only. See the specifications in the product documentation for the required wire size.**
- **See the specifications in the product documentation for the required torque values for the wiring-terminal screws.**

Attention: The following circuit breaker and ground cable ratings apply to -48 V dc power supplies only:

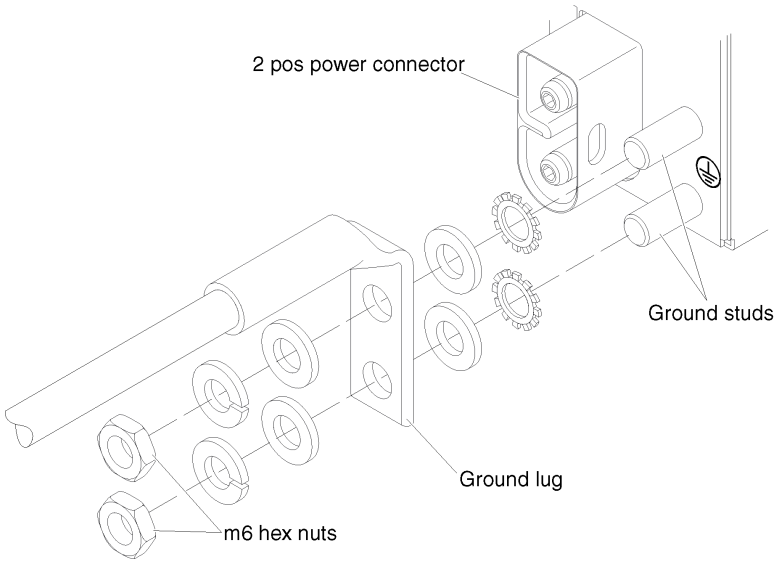
Breaker	Listed 70 A	See Note 1
Ground cable	4 AWG with Listed lug which can accept M6 ground screws	See Note 2
Torque rating for ground screws	4.0 - 4.8 Newton-meters (35.4 - 42.5 inch-pounds)	-

1. The maximum steady state current of the -48 V dc power supply is less then 70 A. However during specific events, such as over subscription, it is possible for the power supply to briefly draw a current greater than 70 A. Therefore it is recommended that the power supply be protected by a Listed circuit breaker that will support up to 90 A for a minimum of 20 ms. The suggested Telect High Current Panel Dual 350A Power Distribution Panel (part number 350CB06) using the Telect 70 A circuit breakers (Part number 090-0052-0070) conforms to this specification.
2. If not connecting to a SELV source which provides Reinforced insulation you must use a Ground Cable.

To connect the chassis to power, complete the following steps:

1. For an ac-powered chassis (**restricted-access location is not required**), connect each power cord from the power supplies to a power distribution unit (PDU), uninterruptible power source (UPS) or wall receptacle. AC power is supplied to the Flex System Enterprise Chassis by one of the following options:
   a. A power cord that connects to a PDU or UPS supplying a maximum 20 A branch circuit protection.
   b. A power cord that connects to a wall receptacle supplying a maximum 20 A branch circuit protection.
   c. A special use Flex System 3X Power Cord that connects to a wall receptacle supplying a maximum 32 A branch circuit protection.

   Attention: Do not route the power cords over removable modules or allow the cords to interfere with the module handles.
2. For dc-powered chassis:
   a. For a chassis powered by -48 to -60 V dc power supplies (**restricted access location is required**), connect an earth ground cable to each power supply.
      1) Use a 10 mm nut driver to remove the hex nuts from the ground studs.
      2) Remove the lock washer and one of the flat washers from each ground stud.
      3) Push the ground lug onto the ground studs; then, place the flat washer, the lock washer, and the hex nut back on each ground stud.
      4) Use a 10 mm nut driver to tighten the hex nuts to 4.0 - 4.8 Newton-meters (35.4 - 42.5 inch-pounds).



   b. Connect each power cord from the dc power supplies to a dc power distribution unit (PDU) (**restricted-access location is not required**).

      Attention:

      - Do not route the power cords over removable modules or allow the cords to interfere with the module handles.
      - In North America, connect the power cords to a UL-listed PDU only.
3. Make sure that the following LEDs are lit:
   - The logo on the chassis front information panel.
   - The dc power and ac power LEDs on each power supply.
   - The power LED on each I/O module.

Note: The power LED on each compute node and on the Flex System Manager management node, if one is installed, flashes slowly to indicate that the node is connected to power and is ready to be turned on.

4. If the LEDs are not lit:
   a. Disconnect the chassis from the power source.
   b. Reseat all of the components in the chassis.
   c. Reconnect the chassis to the power source.
   d. If the problem persists, contact Support.

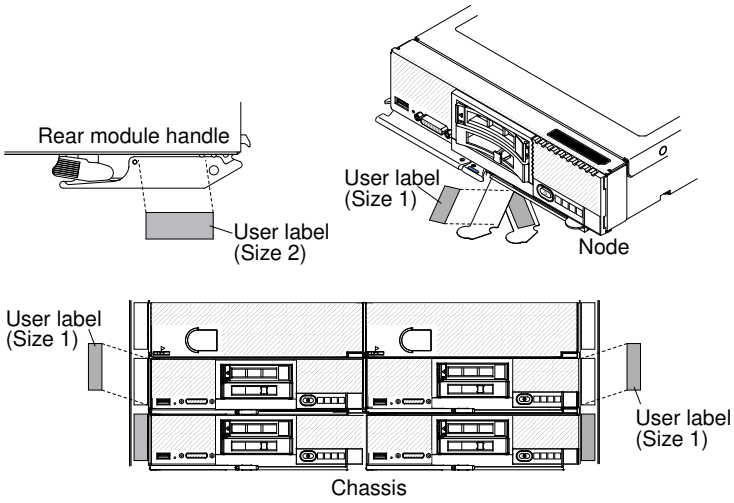
User labels

This section describes the user labels that come with the chassis and shows where to place them.

A set of blank user labels comes with the Flex System Enterprise Chassis. Record the information to identify each installed compute node, storage node, or Flex System Manager management node on the labels and place them on the node label tab and on the adjacent chassis label plate. The large label (size 1) fits on the node label tabs and on the chassis label plates.

Important: Do not place the label directly on the compute node or Flex System Manager management node front bezel or in any way block the ventilation holes.

The small label (size 2) fits on the rear chassis module handles. Use the small labels to record identifying information for the I/O modules and the CMM.



Obtaining firmware updates

You can use the Chassis Management Module or a management node, if installed, to update the chassis firmware.

The following chassis components have firmware that can be updated:

- Chassis Management Module
- Compute nodes
- I/O modules
- Flex System Manager management node

In addition, some of the optional hardware devices that you can order for the chassis have device drivers that you must install.

For example, Ethernet controllers are integrated on each compute node system board. The Ethernet controllers provide 1000 Mbps full-duplex capability only, which enables simultaneous transmission and reception of data to the external ports on the Ethernet switches. You do not have to set any jumpers or configure the controller for the compute node operating system. However, you must install a device driver in the compute node to enable the compute node operating system to address the Ethernet controller.

See the documentation that comes with your optional hardware devices for information about installing any required device drivers.

Attention: Before you install any new components in the Flex System Enterprise Chassis, update the Chassis Management Module firmware to the latest level available. See Updating the CMM firmware"Updating the CMM firmware" in the *Lenovo Flex System Chassis Management Module Installation Guide* for more information.

Using the Chassis Management Module

For more information about using the Chassis Management Module web interface to update the chassis firmware, see Lenovo Flex System Chassis Management Module Chassis management options"Chassis management options" in the *Lenovo Flex System Chassis Management Module User's Guide*.

You can use the Chassis Management Module command-line interface to update the chassis firmware. See Lenovo Flex System Chassis Management Module update command"update command" in the *Lenovo Flex System Chassis Management Module Command-Line Interface Reference Guide* for more information.

Using a management node

If a Lenovo XClarity Administrator is available, you can download, install, and manage firmware updates for managed endpoints, including chassis, compute nodes, and I/O modules. You can assign compliance policies to the managed endpoints to ensure that firmware on those endpoints remains compliant.

Note: Firmware updates can be applied to the hardware only. You cannot update device drivers using the Lenovo XClarity Administrator.

For more information about using the Lenovo XClarity Administrator, see http://flexsystem.lenovofiles.com/help/topic/com.lenovo.lxca.doc/aug_product_page.html.

You can also use the Flex System Manager management node to update firmware and device drivers for all of the chassis components, if one is available. For more information about using the Flex System Manager management software to update firmware and device drivers for the chassis components, see http://flexsystem.lenovofiles.com/help/index.jsp.

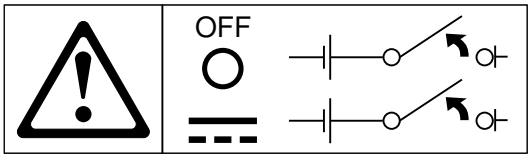
Disconnecting the chassis from power

Follow the instructions in this section to disconnect the Flex System Enterprise Chassis from all power sources.

Before you disconnect the Flex System Enterprise Chassis from power, be sure to follow these instructions to correctly shut down the compute nodes.

Statement 19

CAUTION:
The power-control button on the device does not turn off the electrical current supplied to the device. The device also might have more than one connection to dc power. To remove all electrical current from the device, ensure that all connections to dc power are disconnected at the dc power input terminals.



Statement 31

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 power source.**
- **Connect to properly wired power sources 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 ac power cords, dc power sources, network connections, telecommunications systems, and serial cables before you open the device covers, unless you are instructed otherwise in the installation and configuration procedures.**
- **Connect and disconnect cables as described in the following table when you install, move, or open covers on this product or attached devices.**

To Connect:

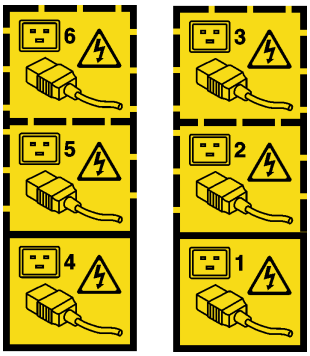
1. Turn OFF all power sources and equipment that is to be attached to this product.
2. Attach signal cables to the product.
3. Attach power cords to the product.
   - For ac systems, use appliance inlets.
   - For dc systems, ensure correct polarity of -48 V dc connections: RTN is + and -48 V dc is -. Earth ground should use a two-hole lug for safety.
4. Attach signal cables to other devices.
5. Connect power cords to their sources.
6. Turn ON all the power sources.

To Disconnect:

1. Turn OFF all power sources and equipment that is to be attached to this product.
   - For ac systems, remove all power cords from the chassis power receptacles or interrupt power at the ac power distribution unit.
   - For dc systems, disconnect dc power sources at the breaker panel or by turning off the power source. Then, remove the dc cables.
2. Remove the signal cables from the connectors.
3. Remove all cables from the devices.

Statement 33

CAUTION:
This device does not provide a power control button. Removing power supply modules or turning off the server blades does not turn off the electrical current supplied to the device. The device also might have more than one power cord. To remove all electrical current from the device, ensure that all power cords are disconnected from the power source.



Attention: The following circuit breaker and ground cable ratings apply to -48 V dc power supplies only:

Breaker	Listed 70 A	See Note 1
Ground cable	4 AWG with Listed lug which can accept M6 ground screws	See Note 2
Torque rating for ground screws	4.0 - 4.8 Newton-meters (35.4 - 42.5 inch-pounds)	-

1. The maximum steady state current of the -48 V dc power supply is less then 70 A. However during specific events, such as over subscription, it is possible for the power supply to briefly draw a current greater than 70 A. Therefore it is recommended that the power supply be protected by a Listed circuit breaker that will support up to 90 A for a minimum of 20 ms. The suggested Telect High Current Panel Dual 350A Power Distribution Panel (part number 350CB06) using the Telect 70 A circuit breakers (Part number 090-0052-0070) conforms to this specification.
2. If not connecting to a SELV source which provides Reinforced insulation you must use a Ground Cable.

To disconnect the chassis from power, complete the following steps:

Step 1. Shut down each compute node. See the documentation that comes with the compute nodes for information about shutting down the operating systems on the compute nodes.

Step 2. Shut down each storage node. See the documentation that comes with the storage node for information about shutting down the node.

Step 3. Shut down the Flex System Manager management node, if one is installed.

Important: If the management node is the active management node in a high-availability configuration (two management nodes), perform a manual failover to the passive management node before you shut down the active management node. See the documentation that comes with the management node for information about high availability and shutting down the management node.

Step 4. Disconnect all power cords on the rear of the chassis from the power source.

Note: After you disconnect the chassis from power, wait at least 5 seconds before you connect the chassis to power again.

Chapter 3. Configuring the Flex System Enterprise Chassis

You can configure the Flex System Enterprise Chassis locally or remotely by using the Chassis Management Module web interface. You must use the CMM to create user accounts and to configure IP addresses for the CMM and the I/O modules before you power-on the Flex System Manager management node, if one is installed. Configuring the chassis involves performing all of the tasks that are necessary to set up a functioning chassis on which you can begin to install applications.

Note: Before you configure the Flex System Enterprise Chassis, make sure that you have completed all installation activities.

To configure the chassis, complete the following tasks:

1. Connect to the CMM web interface to create user accounts and to configure IP addresses for the CMM and the chassis I/O modules (see “Configuring the chassis by using the CMM” on page 65).

   Note:

   - If the chassis does not have a management node available, use the Chassis Management Module web interface to complete the chassis configuration.
   - If you have multiple chassis on the management network, you must establish user accounts and configure the IP addresses using the CMM for each chassis before you power-on the management node, if one is available.
2. If a Lenovo XClarity Administrator is available, use the Lenovo XClarity Administrator to discover and configure the Flex System Enterprise Chassis (see “Configuring the chassis by using the Lenovo XClarity Administrator” on page 69).
3. If a Flex System Manager management node is available, you can connect to the management node and use the setup wizard to configure the management node (see “Configuring the chassis by using the Flex System Manager management node” on page 69).

After you have completed the initial configuration, you can install and configure applications.

Configuring the chassis by using the CMM

Follow the instructions in this section to establish an Ethernet connection to the Chassis Management Module and use the CMM web interface to configure the chassis.

Note:

- You must use the Chassis Management Module to establish user accounts and to configure IP addresses for the CMM and the I/O modules before you power-on the Flex System Manager management node, if one is installed.
- If you have multiple chassis on the management network, you must establish user accounts and configure the IP addresses for each chassis before you power-on the Flex System Manager management node, if one is installed.
- If the chassis does not have an Flex System Manager management node, use the Chassis Management Module web interface to complete the chassis configuration.

For more information about using the Chassis Management Module web interface to configure the chassis, see Lenovo Flex System Chassis Management Module Chassis management options"Chassis management options" in the *Lenovo Flex System Chassis Management Module User's Guide*.

CMM network access tag

Information that you need to initially connect to the CMM is on the network access tag.

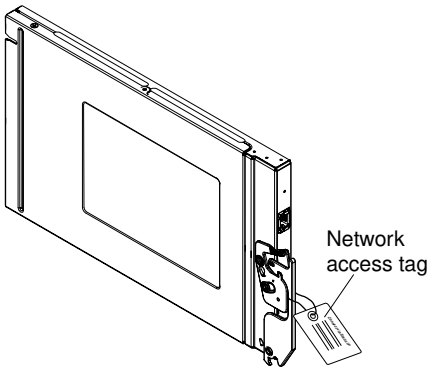
Remove the network access tag from the CMM, before you install the CMM in a Flex System chassis.

The network access tag lists the following initial connection information for the CMM:

- MAC address
- Default host name
- IPv6 link local address (LLA)
- Default URL (IPv4 static IP address): 192.168.70.100
- Default user name (USERID)
- Default password (PASSW0RD, note the number zero, not the letter O, in PASSW0RD

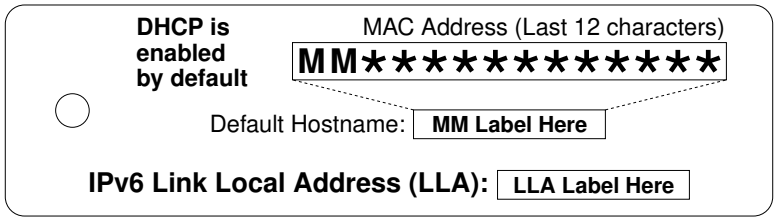
The network access tag is attached to the front of the CMM, as shown in the following illustration.

Note: If DHCP connection (default setting) fails, connection is attempted using the IPv4 static IP address.



The front of the network access tag lists the CMM MAC address, default host name, and IPv6 link local address (LLA), as shown in the following illustration.

Front



The rear of the of the network access tag lists the CMM default URL (IPv4 static IP address), default user name, and default password, as shown in the following illustration.

Rear

IPv6 addressing for initial connection

When you use IPv6 addressing, use the IPv6 link-local address to complete the initial connection to the CMM.

The link-local address is a unique IPv6 address for the CMM that is automatically generated according to its MAC address. It is of the form `FE80::3BA7:94FF:FE07:CBD0`.

Determine the link-local address of the CMM in any of the following ways:

- Read the CMM link-local address on the network access tag that is attached to the front of the CMM (see CMM network access tag"CMM network access tag," in the *Lenovo Flex System Chassis Management Module Command-Line Interface Reference Guide* or *Installation Guide*, for information). Note that the network access tag might have been removed from your CMM during installation.
- If you are able to log in to the CMM command-line interface (CLI) using IPv4 addressing, view the link-local address by using the **ifconfig** command (see Lenovo Flex System Chassis Management Module ifconfig command"ifconfig command" in the *Lenovo Flex System Chassis Management Module Command-Line Interface Reference Guide* for information about command use).
- If you are able to log in to the CMM web interface using IPv4 addressing, view the link-local address on the IPv6 page on the Ethernet page on the Network Protocol Properties page (select **Network** from the **Mgt Module Management** menu). All fields and options are fully described in the CMM web interface online help.

If the CMM does not have a network access tag and you are unable to access the CMM by using IPv4, complete the following steps to calculate link-local address:

Complete the following steps:

Step 1. Write down the MAC address of the CMM. It is on a label on the CMM, near the reset button. The label reads MM*xxxxxxxxxxxx*, where *xxxxxxxxxxxx* is the MAC address. For example:

`39-A7-94-07-CB-D0`

Step 2. Split the MAC address into two parts and insert FF-FE in the middle.For example:

`39-A7-94-`**`FF-FE`**`-07-CB-D0`

Step 3. Convert the two hexadecimal digits at the left end of the string to binary.For example:

- **`39`**`-A7-94-FF-FE-07-CB-D0`
- **`00111001`**`-A7-94-FF-FE-07-CB-D0`

Step 4. Invert the value of bit 7 of the binary string.For example:

- `0011100`**`1`**`1-A7-94-FF-FE-07-CB-D0`
- `0011101`**`1`**`1-A7-94-FF-FE-07-CB-D0`

Step 5. Convert the binary digits at the left end of the string back to hexadecimal.For example:

- **`00111011`**`-A7-94-FF-FE-07-CB-D0`

- **3B**-A7-94-FF-FE-07-CB-D0

Step 6. Combine the hexadecimal digit pairs into 4-digit groups.For example:

- 3B-A7-94-FF-FE-07-CB-D0
- 3BA7-94FF-FE07-CBD0

Step 7. Replace dash (-) separators with colon (:) separators.For example:

- 3BA7-94FF-FE07-CBD0
- 3BA7:94FF:FE07:CBD0

Step 8. Add FE80:: to the left of the string.For example:

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

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

Ethernet connection

Use these instructions to connect to the CMM through an Ethernet connection to use the CMM web interface.

Note: The HTTP connection is not available when the CMM security policy is set to secure (the factory default setting). When the security policy is set to secure, Ethernet connections must be made using HTTPS.

Complete the following steps:

Step 1. Connect an Ethernet cable from the client computer to the CMM by direct connection (Remote management and console connector) or through a network.

Step 2. To connect to the CMM for the first time, you might have to change the Internet Protocol properties on the client computer. Make sure that the subnet of the client computer is set to the same value as the CMM (the default CMM subnet is 255.255.255.0). The IP address of the CMM must also be in the same local domain as the client computer.

Step 3. Open a web browser on the client computer, and direct it to the CMM IP address. You must use a secure connection (https://). For the first connection to the CMM, use the default IP address of the CMM; if a new IP address has been assigned to the CMM, use that one instead.

Note: The factory-defined static IPv4 IP address is 192.168.70.100, the default IPv4 subnet address is 255.255.255.0, and the default host name is MM*xxxxxxxxxxxx*, where *xxxxxxxxxxxx* is the burned-in MAC address. The MAC address is on a label on the CMM, below the IP reset button (see Lenovo Flex System Chassis Management Module CMM controls and indicators"CMM controls and indicators," in the *Lenovo Flex System Chassis Management Module Installation Guide*, for the IP reset button location). See “IPv6 addressing for initial connection” on page 67 for information about determining IPv6 addressing for initial connection.

Step 4. Enter the CMM user name and password to start the remote session.

- The user ID and password are case sensitive. The same user ID and password are used for all methods of connecting to the CMM.
- The default CMM user name is USERID, and the default password is PASSW0RD (note the number zero, not the letter O, in PASSW0RD).

Note: Be sure to set the timeout value you want for your web session.

Step 5. If you are connecting to the Chassis Management Module for the first time, perform initial configuration of the CMM.

Note: Do not restart the CMM using the initial configuration.

Step 6. Set the system-management processor (IMM/FSP) IP addresses for each of the compute nodes in the chassis, including the Flex System Manager management node, if one is installed. From the CMM user interface, select **Chassis Management > Component IP configuration**. Then select the device to change the IP address.

Note:

You must restart each device to show the new IP address.

1. Cable the CMM to the management network and restart the CMM.
2. Configure the Flex System Manager management node Ethernet ports, if a management node is installed:
   a. Use the console breakout cable to connect your client computer (or a keyboard, mouse, and monitor) to the KVM connector on the Flex System Manager management node, if one is installed. See "Connecting to the management node locally by using the console breakout cable" on page 72 for more information.
   b. Start the Flex System Manager management node, if one is installed, and complete the initial setup.

      Note: If you are connecting to a single network for both data and management, configure management node Ethernet port Eth0 only during initial setup. If you are connecting to separate management and data networks, you must configure both management node Ethernet ports Eth0 and Eth1. Make sure that these ports point to networks that are on different subnets.
   c. After completing the management node Ethernet port configuration, you should be able to access the Flex System Manager user interface to complete the setup and begin managing chassis. On a computer connected to the management network, point your web browser to https://*IP_address*, where *IP_address* is the IP address that you entered during initial configuration.
3. Log on to each of the I/O modules in the chassis and configure them.

Configuring the chassis by using the Lenovo XClarity Administrator

After you use the Chassis Management Module to establish user accounts and to configure IP addresses for the CMM and the I/O modules, you can use the Lenovo XClarity Administrator to discover and manage Flex System Enterprise Chassis endpoints.

The Lenovo XClarity Administrator, if available, can discover Flex System chassis, compute nodes, and I/O modules in your environment by probing for manageable systems that are on the same IP subnet as the Lenovo XClarity Administrator. See http://flexsystem.lenovofiles.com/help/topic/com.lenovo.lxca.doc/aug_product_page.html for more information.

Configuring the chassis by using the Flex System Manager management node

After you use the Chassis Management Module to establish user accounts and to configure IP addresses for the CMM and the I/O modules, you can use the Flex System Manager management node to configure the remaining chassis end points, if one is installed. Follow the instructions in this section to establish a connection to the Flex System Manager management node and use the management software to complete the chassis configuration.

Note:

- You must choose the cryptography mode (NIST 800-131A compliant or not) during the FSM setup wizard. The FSM cryptography mode cannot be changed without a fresh installation. See http://

flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.common.nav.doc/nist_implementing_a_compliant_environment.html for more information.

- If the chassis does not have an Flex System Manager management node installed, you must use the CMM to complete the chassis configuration (see "Configuring the chassis by using the CMM" on page 65).

Connect to the Flex System Manager management node in any of the following ways:

- Remotely, using the host name (see "Connecting to the management node remotely by using the host name" on page 70).
- Remotely, using the static IP address (see "Connecting to the management node remotely by using the static IP address" on page 71).
- Locally, using the console breakout cable (see "Connecting to the management node locally by using the console breakout cable" on page 72).

Connecting to the management node remotely by using the host name

Use this information to connect to the Flex System Manager remotely using the hostname and configure the Flex System Enterprise Chassis.

To connect to the Flex System Manager management node remotely by using the host name and configure the Flex System Enterprise Chassis components, complete the following steps:

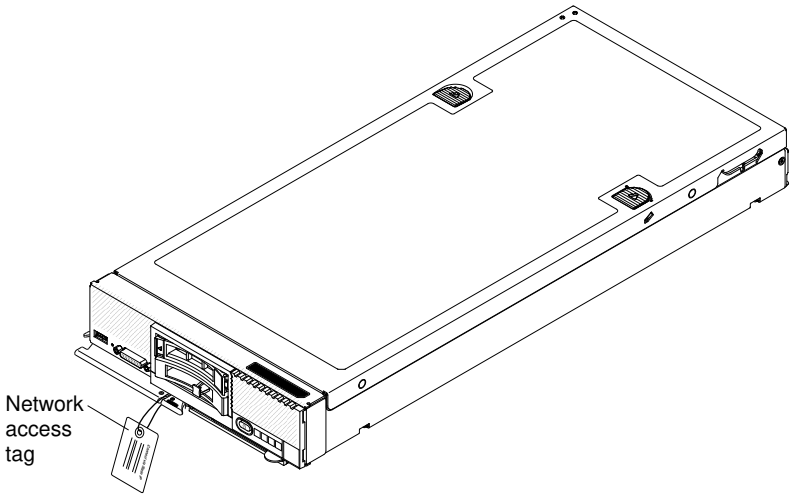
Step 1. Power on the management node.

Step 2. Connect the Ethernet cable from a notebook computer to your management network.

Note:

- The Flex System Manager management node connects to the management network internally via the Chassis Management Module and then to a top-of-rack switch that is used for systems management.
- If there is no DHCP server on the network, Flex System Manager management software will revert back (after 2 minutes) to the static IP address on the network access tag that is attached to the management node. See "Connecting to the management node remotely by using the static IP address" on page 71 for instructions for using the static IP address.

Step 3. Remove the network access tag from the management node. The following illustration shows the location of the Flex System Manager network access tag on the management node.

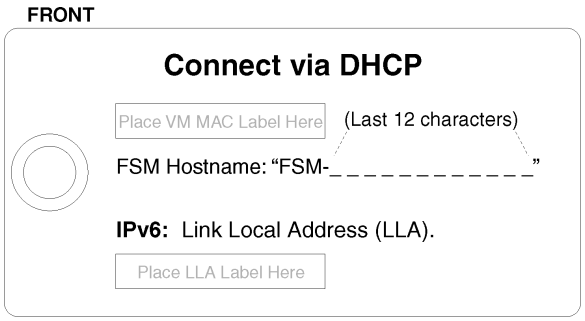


Step 4. Open a web browser.

Step 5. Enter the default host name that is shown on the Flex System Manager network access tag into the web browser address field. For example:

`https://defaulthostname` where `defaulthostname` is `FSM` plus a 12-digit MAC address (`FSM-xxxxxxxxxxx`)

An example of the tag is shown in the following illustration.



Step 6. Log in and accept the license agreement. The configuration wizard starts.

Connecting to the management node remotely by using the static IP address

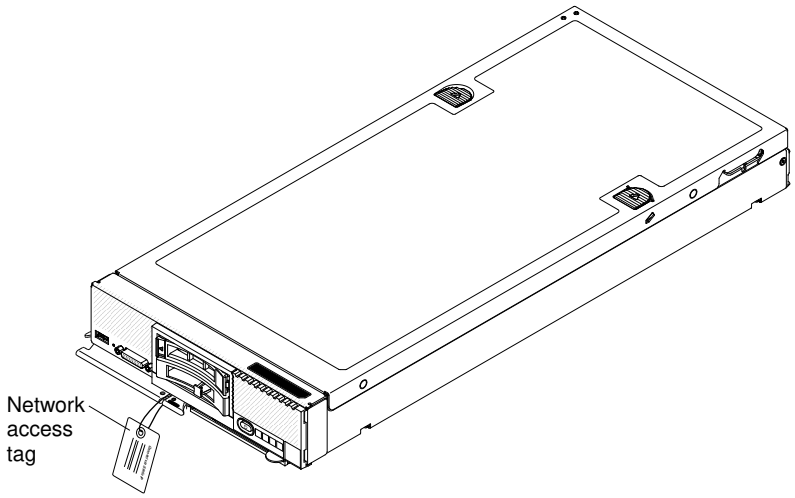
Use this information to connect to the Flex System Manager management node remotely by using the static IP address and configure the Flex System Enterprise Chassis.

The Flex System Manager management node comes with predefined port values that you cannot change. Make sure that the correct ports are open in your firewall before you connect to the management node. See the *Flex System Manager Installation and Service Guide* for information about port availability.

To connect to the Flex System Manager management node remotely and configure the Flex System Enterprise Chassis, complete the following steps:

Step 1. Power on the management node.

Step 2. Make sure that the subnet configuration of the notebook computer is consistent with the subnet mask and IP address that are printed on the network access tag. The following illustration shows the location of the network access tag on the management node.



Step 3. Connect an Ethernet cable from the notebook computer to your management network or directly into the Ethernet connector on the Chassis Management Module in CMM bay 1. See "Connecting to the management node remotely by using the host name" on page 70 for instructions for connecting to the management network.

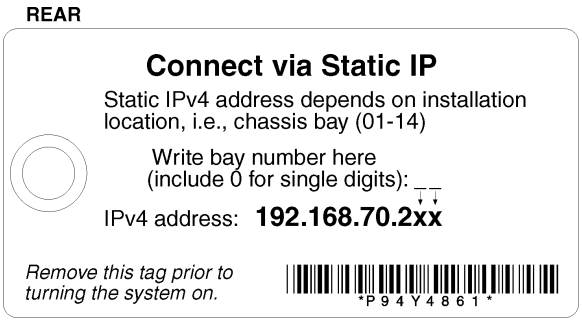
Step 4. Remove the network access tag from the management node.

Step 5. Open a web browser.

Step 6. Enter the IP address that is shown on the network access tag into the web browser address field. The last two digits of the static IP address are based on the node bay in which the management node is installed (for example, use 04 for the last two digits if the management node is in node bay 4). For example:

`https://IPaddress` where the `IPaddress` is `192.168.70.204` (for a management node in node bay 4)

An example of the tag is shown in the following illustration.



Step 7. Log in and accept the license agreement. The configuration wizard starts.

Connecting to the management node locally by using the console breakout cable

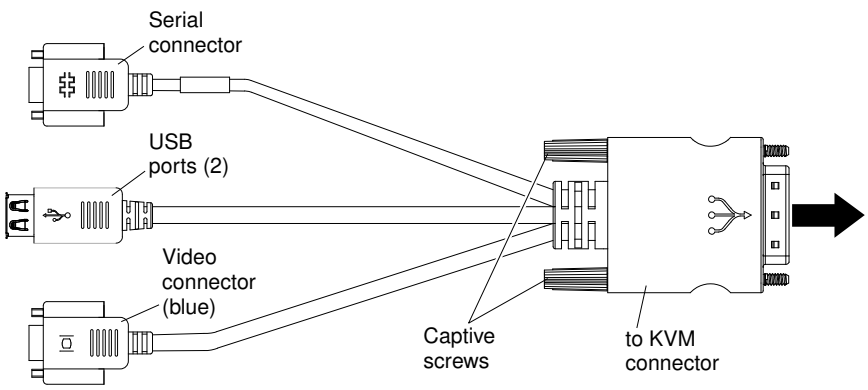
Use this information to connect to the Flex System Manager management node locally by using the console breakout cable and configure the Flex System Enterprise Chassis.

To connect to the Flex System Manager management node locally by using the console breakout cable and configure the Flex System Enterprise Chassis, complete the following steps:

Step 1. Locate the KVM connector on the management node. See the Flex System Manager management node documentation for the location of this connector.

Step 2. Connect the console breakout cable to the KVM connector; then, tighten the captive screws to secure the cable to the KVM connector.

Step 3. Connect a monitor, keyboard, and mouse to the console breakout cable connectors.



Step 4. Power on the management node.

Step 5. Log in and accept the license agreement. The configuration wizard starts.

Configuring the management node

All Flex System Manager management nodes are pre-configured with the same static IP address. The default is 192.168.70.2xx. The last two digits (*xx*) in the static IP address are the bay number in which the compute node is installed in the chassis. For example, if the compute node is installed in bay 2, the value of *xx* in the static IP address is 02. You can use the Flex System Manager management software to assign a new static IP address.

Important:

- If you are installing two management nodes in separate chassis of a multiple-chassis configuration, they must *not* be installed in the same node bay. For example, if you install the first management node in node bay 1 of one chassis, install the second management node in any available node bay other than node bay 1 in a *different* chassis.
- The management nodes default static IP address depends in part on the node bay that it is installed in. If you install two management nodes in the same node bay in different chassis in a multiple-chassis configuration, they will have the same default IP address.
- Configure one management node at a time.

To establish connectivity, the management node attempts to use Dynamic Host Configuration Protocol (DHCP) to acquire its initial IP address for the Chassis Management Module Ethernet port. If DHCP is not installed or is enabled and fails, the management node uses the static IP address. Use the Flex System Manager management software to configure other chassis component settings, such as user accounts, DHCP, or Wake on LAN.

For more information, see the *Flex System Manager Installation and Service Guide*.

Configuring I/O modules

Use the Chassis Management Module web interface to configure ports and IP addresses for the I/O modules in the Flex System Enterprise Chassis.

You must enable at least one external port on an Ethernet switch module in I/O module bay 1 or 2 to communicate with the Ethernet controllers that are integrated in each compute node. See the documentation that comes with the I/O module for information about configuration. I/O module information is available at http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.networkdevices.doc/network.html.

Note: If a pass-thru module is installed in I/O module bay 1, you must configure the network switch that the pass-thru module is connected to. See the documentation that comes with the network switch for more information. See “Network integration with the Flex System Manager” on page 52 for diagrams of the chassis management and data networks.

To determine which I/O modules are compatible with the Flex System Enterprise Chassis, see http://www.lenovo.com/serverproven/.

Port mapping

Table 8 “I/O bay to expansion adapter port mapping” on page 74 summarizes the Flex System Enterprise Chassis I/O bay and port interconnections for each network switch and adapter. In this table, the bay numbers correspond to the I/O bay in the chassis. Installing a second network switch in the chassis enables a redundant path and a separate connection from the compute node (or other device) to the external devices on the network. The second switch port connection in Table 8 “I/O bay to expansion adapter port mapping” on page 74 allows for dual paths from the compute node (or other device) to external devices.

Table 8. I/O bay to expansion adapter port mapping

Chassis I/O bay	Compute node I/O expansion adapter port
1	Port 0 connection on the I/O expansion adapter in compute node position 1
2	Port 1 connection on the I/O expansion adapter in compute node position 1
3	Port 0 connection on the I/O expansion adapter in compute node position 2
4	Port 1 connection on the I/O expansion adapter in compute node position 2

The node in bay 1 in Figure 1 “ LOM, I/O adapter, and network switch connections” on page 74 shows that when a compute node is shipped with a LAN on motherboard (LOM) connector, the LOM connector provides the link from the node system board to the chassis midplane. If required, the LOM connector can be removed from the compute node and an I/O expansion adapter can be installed in the node. A compute node with an I/O expansion adapter installed is shown in bay 2 in Figure 1 “ LOM, I/O adapter, and network switch connections” on page 74.

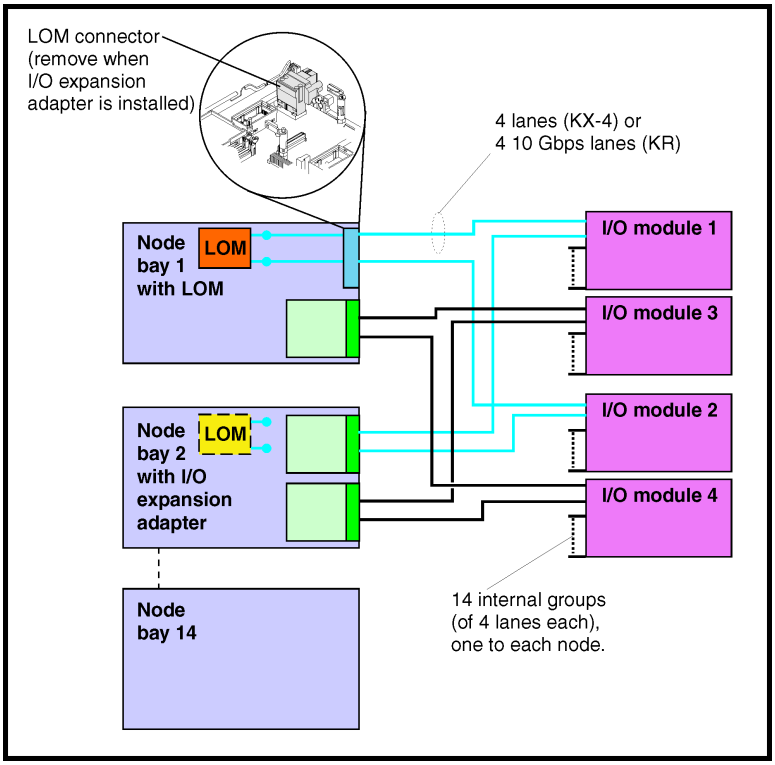


Figure 1. LOM, I/O adapter, and network switch connections

A total of two I/O expansion adapters (M1 and M2 in Figure 2 “ Logical layout of node-to-switch interconnections” on page 75) can be installed in a 1-bay compute node. Up to four I/O expansion adapters can be installed in a 2-bay compute node.

Each I/O expansion adapter has two connectors, one connects to the node system board and the second connector is a high-speed interface that connects to the midplane when the node is installed in the chassis.

As shown in Figure 2 “ Logical layout of node-to-switch interconnections” on page 75, each of the links to the chassis midplane (shown in blue) are four links wide. The exact number of links used on each I/O expansion adapter is dependent on the type of application-specific integrated circuit (ASIC) that is installed and the number of ports that are wired.

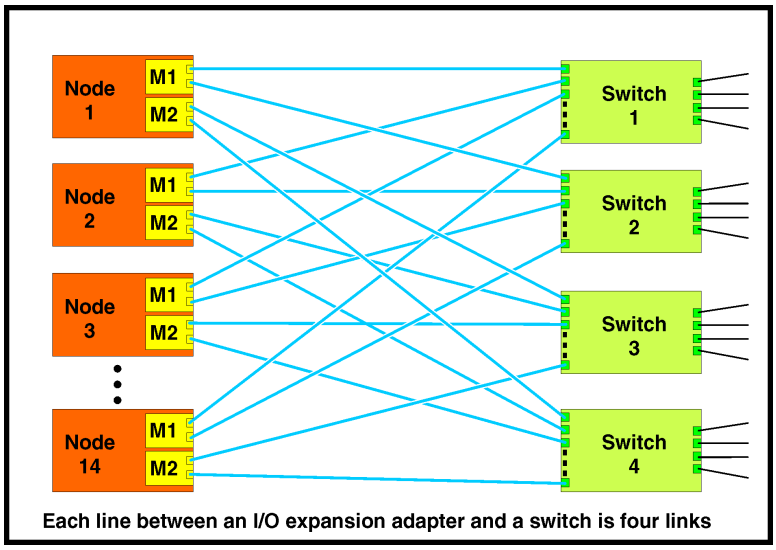


Figure 2. Logical layout of node-to-switch interconnections

Configuring compute nodes

After you use the Chassis Management Module to establish user accounts and to configure IP addresses for the CMM and the I/O modules, you can use the Flex System Manager management node to configure the compute nodes, if one is installed.

Note: If the chassis does not have a Flex System Manager management node installed, you must use the CMM to configure the compute nodes. See "Configuring the chassis by using the CMM" on page 65 for more information.

Configuring a compute node involves installing the operating system and updating the firmware. See the documentation that comes with your compute node for configuration information. For more information about compute nodes, see http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.common.nav.doc/compute_blades.html.

To determine which compute nodes are compatible with the Flex System Enterprise Chassis, see http://www.lenovo.com/serverproven/.

For more information about using the Flex System Manager to configure compute nodes, see the *Flex System Manager Installation and Service Guide*.

Chapter 4. Troubleshooting the chassis

If you experience problems with your Flex System Enterprise Chassis, there are several ways to isolate and solve the problem.

Using a management node

If a Lenovo XClarity Administrator or Flex System Manager management node is available, always use it as the starting point for troubleshooting the chassis. The management node communicates directly with the compute nodes and I/O modules and can aggregate status and logs from multiple chassis.

If no management node is available, you can use the Flex System Chassis Management Module (CMM) for troubleshooting.

Note: If you are using a Flex System Manager management node, a failed CMM might not allow monitoring of chassis components. If a Flex System Manager is installed in a chassis without a working CMM, the Flex System Manager might not be able to reach the network to monitor other devices because it uses a network path through the CMM. For this reason, a chassis that contains a Flex System Manager should also contain two CMMs. The primary CMM automatically fails over to the standby CMM if there is a monitoring problem or a problem with the CMM.

Using the Flex System Chassis Management Module

Status information about fan modules, power supplies, and CMMs comes from the CMM. The CMM can also report some hardware errors on the I/O modules and compute nodes. The CMM is not operating-system aware and does not have information about device drivers.

The CMM allocates power to components and provides power permission to compute nodes if enough power is available. I/O modules are automatically powered on by the CMM if enough power is available. The CMM does not turn off power to I/O modules or compute nodes. The I/O modules and compute nodes have their own firmware that protects the hardware.

A service-level reset command is available in the CMM command-line interface that you can use to remotely cycle power to a monitored component. A service-level reset is a useful substitute for physically reseating a component, because it restarts the component without requiring physical access. See Lenovo Flex System Chassis Management Module service command"service command" in the *Lenovo Flex System Chassis Management Module Command-Line Interface Reference Guide* for more information.

See also Lenovo Flex System Chassis Management Module service and support options"Service and support options" in the *Lenovo Flex System Chassis Management Module User's Guide*.

Using the diagnostic LEDs

The front information panel has a fault (yellow) LED, a check log (yellow) LED, and an identify (blue) LED. If any LED is lit, it indicates that the chassis has power. Any lit yellow LED on the chassis indicates to log in to the highest level management device that is available (Flex System Manager management node or CMM) and read the event log. The identify LED is used to help identify the location of the failed component or chassis. Blue LEDs are always a result of a user action.

Service bulletins

The Support website is continually with tips and techniques that you can use to solve problems that you might have with the Flex System Enterprise Chassis.

To find service bulletins that are available for the Flex System Enterprise Chassis, go to http://support.lenovo.com and search for the terms `Flex System` and `retain`.

Diagnostic tools

This section provides information about specific diagnostic tools that you can use to diagnose and solve hardware-related problems.

CMM event log

The CMM event log contains a list of all events that are received from all devices in the Flex System Enterprise Chassis. These events are also sent by the CMM to the Flex System Manager, if a management node is installed.

You can view the Chassis Management Module event log by using the CMM command-line interface `displaylog` command, through the CMM web interface, or by viewing the Flex System Manager event log.

Note: Communications errors from the compute nodes can take up to 20 minutes to appear in the CMM event log.

When you read the CMM event log, the most recent events are displayed first. There are user responses in each of the event messages. The user response is intended to resolve problems that are active events. However, there are cases where the problem might have recovered without intervention. If the problem is not an active event, there might be a log entry indicating that it has already recovered. Before you perform the tasks indicated in the user response, verify that the problem remains an active event. If it is not an active event, look for a log entry that indicates it has recovered.

When an error condition has recovered, the event log entry for the recovery will contain the same event id, description, and user action as the original event. You must read the event text to determine if the message is a recovery event or a problem event.

For example, the problem statement for event 000A6001 is: `Fan module %s is operating in a degraded state.`

The recovery statement for event 000A6001 is: `Fan module %s has returned to normal speed operation.`

Unresolved problems will be regenerated if they still exist. For example, if there was a CMM failover or restart, the active events list will be recreated. Note also that the CMM log does not refresh.

Attention: Before troubleshooting the Flex System Enterprise Chassis, make sure that the CMM firmware is the latest level available. Often problems have already been corrected and the fix is available with a firmware update. See Updating the CMM firmware"Updating the CMM firmware" in the *Lenovo Flex System Chassis Management Module Installation Guide* for more information.

For each event code, the following fields are displayed:

Event identifier

An eight-character hexadecimal identifier that uniquely identifies an event or class of events. Event identifiers are displayed in the event log and in notifications (emails and SNMP alerts).

Note: In SNMP alerts, the event identifier is displayed as a decimal number. You convert that integer into a hexadecimal number to map it to the event that is displayed in this document.

Event description

The logged message string that appears for an event. The logged message string that appears in this document is slightly different from the event string that appears in the event log.

When the event string is displayed in the event log, information such as a user ID or a specific node bay number is displayed. In this document, that additional information appears as [arg#].

Explanation

Provides additional information to explain why the event occurred.

Severity

An indication of the level of concern for the condition. In the event log severity is abbreviated to the first character. The following table describes the severity levels.

Table 9. Severity levels

The severity levels table is a two-column table that explains the severity levels of CMM events. Column 1 lists the severity level. Column 2 describes the severity level.

Severity	Description
Informational	An informational message is information that is recorded for audit purposes, usually a user action or a change of states that is normal behavior.
Warning	A warning is not as severe as an error, but if possible, you should correct the condition before it becomes an error. It might also be a condition that requires additional monitoring or maintenance.
Error	An error typically indicates a failure or critical condition that impairs service or an expected function.

Alert category

Similar events are grouped together in categories. Information in the alert category field is displayed as *component* (*severity*).

component

Events are grouped into the following component categories:

- Compute node
- Chassis/System Management
- Cooling devices
- I/O modules
- Inventory
- Network change
- Power supplies
- Power on/off

In addition, the following categories are available:

- *Event log:* Events related to the event log. For example, if the field Monitor log state events is enabled on the Event log page of the Chassis Management Module Web interface, events related to the log being 75% full and the log being 100% full are listed for this category.
- *User activity:* Audit related events, such as when a user logs in to the Chassis Management Module Web interface.

severity

Events are also grouped into the following severity levels:

- Informational
- Warning
- Critical

Note: The severity Critical for the Alert Category field is the same as the severity Error in the Severity field.

Log source

Use the log source as an aid in determining which component has reported an event. The log source field shows one of the following sources:

- Audit. A user action log.
- Node_*number*. The compute node indicated by the bay number.
- Cool_*number*. A fan module indicted by bay number.
- IOMod_*number*. An I/O module indicated by the bay number.
- Power_*number* . A power supply indicated by the bay number.
- SERVPROC. The system-management processor for the CMM.

Automatically notify service

If this field is set to “Yes,” and you have enabled Electronic Service Agent on the Flex System Manager, Support will be notified automatically if the event is generated.

While waiting for Support to call, you can perform the recommended actions for the event.

Recoverable

If this field is a “Yes,” it indicates that the CMM can generate a message that shows the condition has recovered. This does not mean that the event is a recovery of the condition.

If the message is a recovery message, the CMM will typically prefix the message with the word “Recovery”. An example of a recoverable message is an over- temperature threshold event. A component alerts the CMM for an over-temperature condition and then recovers when the condition no longer exists.

If this field is a “No” then there is no possible recovery reported by the CMM. These are typically informational message such as a user has logged in, or a component was installed.

Chassis LEDs that are lit

Where appropriate, this field displays the chassis LEDs that are lit for an event. The front panel of a chassis provides LED indicators for power, faults, location, and a check logs indicator. Some events will cause an LED to illuminate. Other events, such as events from a compute node, are indicated through the chassis as well as through LEDs on the compute node. For example, if a compute node error LED is lit, the chassis error LED should also be lit.

For more information about chassis LEDs, see “Front information panel LEDs” on page 926 and “Chassis module LEDs” on page 928.

SNMP Trap ID

The SNMP trap ID found in the SNMP alert management information base (MIB).

SNMP users will be notified of the alerts in the event categories via an SNMP trap. The traps are defined in mmalert.mib, which is distributed with the Chassis Management Module firmware. The following table shows the MIB Object and the Object Identifier (OID) for the selected alert category.

The SNMP trap ID table is a three-column table that shows the MIB Object and the Object Identifier (OID) for SNMP alert categories. Column 1 lists the alert categories. Column 2 identifies the associated MIB object. Column 3 lists the object identifier.

Alert categories	MIB object	Object identifier
Critical/Error		
Chassis/System Management (Critical)	mmTrapChassisC	.1.3.6.1.4.1.2.6.158.3.0.130
Cooling devices (Critical)	mmTrapFanC	.1.3.6.1.4.1.2.6.158.3.0.133
Power supplies (Critical)	mmTrapPsC	.1.3.6.1.4.1.2.6.158.3.0.4
Nodes (Critical)	mmTrapBladeC	.1.3.6.1.4.1.2.6.158.3.0.128
I/O modules (Critical)	mmTrapIOC	.1.3.6.1.4.1.2.6.158.3.0.129
Storage modules (Critical)	mmTrapStorageC	.1.3.6.1.4.1.2.6.158.3.0.131
NonCritical/Warning		
Chassis/System Management (Warning)	mmTrapChassisN	.1.3.6.1.4.1.2.6.158.3.0.162
Cooling devices (Warning)	mmTrapFanN	.1.3.6.1.4.1.2.6.158.3.0.165
Power supplies (Warning)	mmTrapPowerN	.1.3.6.1.4.1.2.6.158.3.0.164
Nodes (Warning)	mmTrapBladeN	.1.3.6.1.4.1.2.6.158.3.0.160
I/O modules (Warning)	mmTrapION	.1.3.6.1.4.1.2.6.158.3.0.161
Storage Modules (Warning)	mmTrapStorageN	.1.3.6.1.4.1.2.6.158.3.0.163
Event Log (Warning)	mmTrapLogFullN	.1.3.6.1.4.1.2.6.158.3.0.7
System/Informational		
Chassis/System Management (Informational)	mmTrapChassisS	.1.3.6.1.4.1.2.6.158.3.0.178
Cooling devices (Informational)	mmTrapFanS	.1.3.6.1.4.1.2.6.158.3.0.181
Power supplies (Informational)	mmTrapPowerS	.1.3.6.1.4.1.2.6.158.3.0.180
Nodes (Informational)	mmTrapBladeS	.1.3.6.1.4.1.2.6.158.3.0.176
I/O modules (Informational)	mmTrapIOS	.1.3.6.1.4.1.2.6.158.3.0.177
Storage modules (Informational)	mmTrapStorageS	.1.3.6.1.4.1.2.6.158.3.0.179
Event log (Informational)	mmTrapSysLogS	.1.3.6.1.4.1.2.6.158.3.0.35
Power on/off (Informational)	mmTrapPwrDOS	.1.3.6.1.4.1.2.6.158.3.0.182
Inventory change (Informational)	mmTrapSysInvS	.1.3.6.1.4.1.2.6.158.3.0.34
Network change (Informational))	mmTrapNwChangeS	.1.3.6.1.4.1.2.6.158.3.0.37
User activity (Informational)	mmTrapRemoteLoginS	.1.3.6.1.4.1.2.6.158.3.0.30
Test message	mmTrapAppS	.1.3.6.1.4.1.2.6.158.3.0.22

User response

Indicates what actions you should perform to resolve the event. Perform the steps listed in this section in the order shown until the problem is resolved.

If, after performing all of the actions described in the User Response, you cannot resolve the problem, you can submit an Electronic Service Request. Submitting an Electronic Service Request will start the

process of determining a solution to your problem by making the pertinent information available to Support.

Note: If the *call home* capability is enabled (CMM Service Advisor or Flex System Manager Electronic Service Agent), the management device can automatically report serviceable events to Support and provide the associated system service information.

You can also go to http://support.lenovo.com to manually submit an Electronic Service Request.

Note: This list includes error codes and messages that will only appear when certain chassis settings or options are installed.

List of CMM events

This section lists all messages that can be sent from the CMM.

- **00000014 : Test alert was generated by user ID [arg1].**

  The Chassis Management Module has sent a test message to help verify connectivity.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Test Message

  SNMP Trap ID
  mmTrapAppS

  CIM Information
  Prefix: CMM **ID:** 0003

  User Response
  Information only; no action is required.

- **0000006B : The [arg1] log is full.**

  The Chassis Management Module log specified in [arg1] is full. The specified log can be "system" or "audit". New entries in the specified log will overwrite the oldest entries. Log fullness monitoring is disabled by default and must be enabled by the user. The syslog can be use to collect a larger history of log messages on a remote server.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Event Log (Warning)

  SNMP Trap ID
  mmTrapLogFullN

CIM Information
Prefix: CMM **ID:** 0395

User Response
Save the log, solve open problems, and then clear the log.

- **00000071 : The [arg1] log is almost full.**

The Chassis Management Module log specified in [arg1] is 75% full. The specified log can be "system" or "audit". When the specified log is completely full, new entries in the log will overwrite the oldest entries. Log fullness monitoring is disabled by default and must be enabled by the user. The syslog can be use to collect a larger history of log messages on a remote server.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Event Log (Informational)

SNMP Trap ID
mmTrapSysLogS

CIM Information
Prefix: CMM **ID:** 0399

User Response
Information only; no action is required.

- **0000007A : Login successful. User ID [arg1] from [arg2] at IP address [arg3].**

The specified user has logged in to the Chassis Management Module.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0001

User Response
Information only; no action is required.

- **0000016B : The [arg1] log is full.**

The Chassis Management Module log specified in [arg1] is full. The specified log can be "system" or "audit". New entries in the specified log will overwrite the oldest entries. Log fullness monitoring is disabled by default and must be enabled by the user. The syslog can be use to collect a larger history of log messages on a remote server.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Event Log (Warning)

SNMP Trap ID
mmTrapLogFullN

CIM Information
Prefix: CMM **ID:** 0395

User Response
Save the log, solve open problems, and then clear the log.

- **00000171 : The [arg1] log is almost full.**

  The Chassis Management Module log specified in [arg1] is 75% full. The specified log can be "system" or "audit". When the specified log is completely full, new entries in the log will overwrite the oldest entries. Log fullness monitoring is disabled by default and must be enabled by the user. The syslog can be use to collect a larger history of log messages on a remote server.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Event Log (Informational)

  SNMP Trap ID
  mmTrapSysLogS

  CIM Information
  Prefix: CMM **ID:** 0399

  User Response
  Information only; no action is required.

- **0000017A : Monitoring the fullness of the Chassis Management Module system and audit logs has been enabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has enabled monitoring of the fullness state of the Chassis Management Module system and audit logs.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category

User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0675

User Response
Information only; no action is required.

- **0000017B : Monitoring the fullness of the Chassis Management Module system and audit logs has been disabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has disabled monitoring of the fullness state of the Chassis Management Module system and audit logs.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0676

  User Response
  Information only; no action is required.

- **00006011 : The battery in Chassis Management Module [arg1] is low.**

  The battery in the Chassis Management Module is failing.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0818

  User Response
  Replace the battery.

- **00006012 : The battery in Chassis Management Module [arg1] is low.**

  The battery in the Chassis Management Module is failing.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Chassis/System Management (Critical)

SNMP Trap ID
mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0818

User Response
Replace the battery.

- **00006120 : Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.**

  FPGA Host communication is offline.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0819

  User Response
  Complete the following steps until the problem is solved:
  - Reseat Chassis Management Module.
  - Replace the Chassis Management Module.

- **00006121 : Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.**

  FPGA Host communication is offline.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0819

User Response
Complete the following steps until the problem is solved:
- Reseat Chassis Management Module.
- Replace the Chassis Management Module.

- **00006122 : Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.**

FPGA Host communication is offline.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Chassis/System Management (Critical)

SNMP Trap ID
mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0819

User Response
Complete the following steps until the problem is solved:
- Reseat Chassis Management Module.
- Replace the Chassis Management Module.

- **00006123 : Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.**

FPGA Host communication is offline.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Chassis/System Management (Critical)

SNMP Trap ID
mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0819

User Response
Complete the following steps until the problem is solved:
- Reseat Chassis Management Module.
- Replace the Chassis Management Module.

- **00006124 : Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.**

FPGA Host communication is offline.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Chassis/System Management (Critical)

SNMP Trap ID
mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0819

User Response
Complete the following steps until the problem is solved:
- Reseat Chassis Management Module.
- Replace the Chassis Management Module.

- **00006125 : Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.**

  FPGA Host communication is offline.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0819

  User Response
  Complete the following steps until the problem is solved:
  - Reseat Chassis Management Module.
  - Replace the Chassis Management Module.

- **00006126 : Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.**

  FPGA Host communication is offline.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

SNMP Trap ID
mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0819

User Response
Complete the following steps until the problem is solved:
- Reseat Chassis Management Module.
- Replace the Chassis Management Module.

- **00006220 : Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.**

  FPGA Host communication is offline.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0819

  User Response
  Complete the following steps until the problem is solved:
  - Reseat Chassis Management Module.
  - Replace the Chassis Management Module.

- **00006221 : Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.**

  FPGA Host communication is offline.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0819

  User Response
  Complete the following steps until the problem is solved:
  - Reseat Chassis Management Module.
  - Replace the Chassis Management Module.

- **00006222 : Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.**

FPGA Host communication is offline.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Chassis/System Management (Critical)

SNMP Trap ID
mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0819

User Response
Complete the following steps until the problem is solved:
- Reseat Chassis Management Module.
- Replace the Chassis Management Module.

- **00006223 : Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.**

FPGA Host communication is offline.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Chassis/System Management (Critical)

SNMP Trap ID
mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0819

User Response
Complete the following steps until the problem is solved:
- Reseat Chassis Management Module.
- Replace the Chassis Management Module.

- **00006224 : Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.**

FPGA Host communication is offline.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Chassis/System Management (Critical)

SNMP Trap ID
mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0819

User Response
Complete the following steps until the problem is solved:
- Reseat Chassis Management Module.
- Replace the Chassis Management Module.

- **00006225 : Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.**

  FPGA Host communication is offline.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0819

  User Response
  Complete the following steps until the problem is solved:
  - Reseat Chassis Management Module.
  - Replace the Chassis Management Module.

- **00006226 : Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.**

  FPGA Host communication is offline.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0819

  User Response
  Complete the following steps until the problem is solved:

- Reseat Chassis Management Module.
- Replace the Chassis Management Module.

- **00010022 : Chassis Management Module failed to obtain DHCP IP address.**

  The Chassis Management Module cannot obtain an IP address from the DHCP server.

  Severity
  Informational

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0373

  User Response
  Complete the following steps until the problem is solved:

  1. Make sure that the Ethernet cable is connected and devices on both ends of the cable are functioning.
  2. Make sure that the DHCP server is up and running.

- **00014035 : File [arg1] was deleted by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has deleted the specified file from the Chassis Management Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0630

  User Response
  Information only; no action is required.

- **00014041 : CIN node pair (VLAN ID [arg1] and IP address [arg2]) was enabled by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has enabled the specified chassis internal network (CIN) node pair.

  Severity
  Informational

  Serviceable

No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0963

User Response
Information only; no action is required.

- **00014042 : CIN node pair (VLAN ID [arg1] and IP address [arg2]) was disabled by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has disable the specified chassis internal network (CIN) node pair.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0964

  User Response
  Information only; no action is required.

- **00014043 : CIN node pair (VLAN ID [arg1] and IP address [arg2]) was added by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has added the specified chassis internal network (CIN) node pair.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0965

User Response
Information only; no action is required.

- **00014044 : CIN node pair (VLAN ID [arg1] and IP address [arg2]) was deleted by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has deleted the specified chassis internal network (CIN) node pair.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0966

  User Response
  Information only; no action is required.

- **00014045 : CIN node pair (VLAN ID [arg1] and IP address [arg2]) was changed by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed one or both chassis internal network (CIN) parameters for the node. These parameters include the CIN VLAN ID and the CIN IP address.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0967

  User Response
  Information only; no action is required.

- **00014046 : Global enablement CIN by user ID [arg1] from [arg2] at IP address [arg3] was successful.**

  The specified user has enabled successfully the chassis internal network (CIN) for all configured nodes.

  Severity
  Informational

  Serviceable
  No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0968

User Response
Information only; no action is required.

- **00014047 : Global disablement of CIN by user ID [arg1] from [arg2] at IP address [arg3] was successful.**

  The specified user has disabled successfully the chassis internal network (CIN). All CIN functions are disabled for all configured nodes.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0969

  User Response
  Information only; no action is required.

- **00014048 : Global enablement of CIN by user ID [arg1] from [arg2] at IP address [arg3] failed.**

  The specified user has failed to enable the chassis internal network (CIN) for all configured nodes.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0970

  User Response
  Information only; no action is required.

- **00014049 : Global disablement of CIN by user ID [arg1] from [arg2] at IP address [arg3] failed.**

  The specified user has failed to disable the chassis internal network (CIN). All CIN functions are still enabled for all configured nodes.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0971

  User Response
  Information only; no action is required.
- **0001404A : IPv6 was enabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has enabled IPv6 support on the Chassis Management Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0950

  User Response
  Information only; no action is required.
- **0001404B : IPv6 was disabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has disabled IPv6 support on the Chassis Management Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0951

User Response
Information only; no action is required.

- **0001404C : IPv6 static configuration was enabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has enabled IPv6 static address assignment on the Chassis Management Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0952

  User Response
  Information only; no action is required.

- **0001404D : IPv6 static configuration was disabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has disabled IPv6 static address assignment on the Chassis Management Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0953

  User Response
  Information only; no action is required.

- **0001404E : IPv6 static configuration for [arg1] CMM is changed, gateway=[arg2] prefix length= [arg3], IP address = [arg4] by user ID [arg5] from [arg6] at IP address [arg7].**

  The specified user has changed the IPv6 static address configuration on the Chassis Management Module.

  Severity

Informational

Serviceable
No

Automatically notify support
No

Alert Category
Network change (Informational)

SNMP Trap ID
mmTrapNwChangeS

CIM Information
Prefix: CMM **ID:** 0566

User Response
Information only; no action is required.

- **00014053 : IPv6 DHCP address configuration is enabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has enabled DHCPv6 on the Chassis Management Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0567

  User Response
  Information only; no action is required.

- **00014054 : IPv6 DHCP address configuration is disabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has disabled DHCPv6 on the Chassis Management Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0568

User Response
Information only; no action is required.

- **00014055 : DHCPv6 IP address for [arg1] CMM was not obtained because the DHCP timeout period was exceeded.**

  The Chassis Management Module was not able to obtain a dynamic address assignment from DHCPv6.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0569

  User Response
  Complete the following steps until the problem is solved:

  1. Make sure that the Ethernet cable is connected and the devices on both ends of the cable are functioning.
  2. Make sure that the DHCPv6 server is up and running.

- **00014056 : DHCPv6 configuration for [arg1] CMM has been enabled: DN=[arg2], IP=[arg3], prefix=[arg4], DNS1=[arg5].**

  The specified DHCPv6 configuration is currently enabled for the Chassis Management Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0571

  User Response
  Information only; no action is required.

- **00014060 : IPv6 stateless address auto-configuration is enabled by user ID [arg1] from [arg2] at IP address [arg3].**

The specified user has enabled IPv6 stateless address auto-configuration on the Chassis Management Module.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0776

User Response
Information only; no action is required.

- **00014061 : IPv6 stateless address auto-configuration is disabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has disabled IPv6 stateless address auto-configuration on the Chassis Management Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0777

  User Response
  Information only; no action is required.

- **00015011 : Automated file transfer problem reporting configuration was not changed by user ID [arg1] from [arg2] at IP address [arg3].**

  The configuration of the automated file transfer problem report cannot be changed because one or more configuration settings are not valid.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0351

User Response
Correct the configuration settings (including all passwords) and attempt to save the configuration again.

- **00015012 : Automated file transfer problem report configuration changed by user ID [arg1] from [arg2] at IP address [arg3].**

The specified user has changed the configuration for the automated file transfer report for service data.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0352

User Response
Information only; no action is required.

- **00015013 : Automated file transfer of service data via [arg1] failed for event [arg2].**

The file transfer of service data for an automatic support notification was not successful.

Severity
Informational

Serviceable
Yes

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0353

User Response
Complete the following steps until the problem is solved:

1. Ping the FTP server to make sure that it is functional.

2. Make sure that the FTP server exists and is configured correctly.
3. Attempt to log in to the FTP server.
4. Determine whether there is a problem with the firewall between the Chassis Management Module and the FTP server.
5. Manually save the service data.

- **00015014 : Manual email of service information [arg1] reported by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user attempted an email notification, and the notification was successfully reported or failed to be reported.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0354

  User Response
  Information only; no action is required.

- **00015050 : Service data collection for event [arg1] failed. Service event will not be reported.**

  Service data was not collected for the specified event, and an automatic support notification was not attempted.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0357

  User Response
  Submit a service request for the event.

- **00015060 : Call home exclusion list modified by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has changed the exclusion list for automatic support notifications.

  Severity

Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0358

User Response
Information only; no action is required.

- **00015070 : The call home of event [arg1] is canceled. The event recovered before notification was sent.**

  An event was queued as an automatic support notification, but the error was corrected before the notification was sent. The notification has not been sent.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0116

  User Response
  Information only; no action is required.

- **00015100 : Firmware update of [arg1] started by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has started a firmware update of the specified device.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0068

User Response
Information only; no action is required.

- **00015101 : Firmware update of device [arg1] complete. Build ID: [arg2].**

The specified firmware update has been completed.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0069

User Response
Information only; no action is required.

- **00015102 : Firmware update of device [arg1] failed. Reason: [arg2].**

The specified firmware has not been updated.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0070

User Response
The firmware update was not completed normally. If the target image was partially written, another message is displayed. To update the firmware to the target level, update the firmware again. If event message indicates incompatible key, acquire the correct firmware version for a Chassis Management Module and retry the firmware update operation.

- **00015105 : Firmware update of device [arg1] complete. Build ID: [arg2].**

The specified firmware update has been completed.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0069

User Response
Information only; no action is required.

- **00015106 : Firmware update of device [arg1] failed. Reason: [arg2].**

The specified firmware has not been updated.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0070

User Response
The firmware update was not completed normally. If the target image was partially written, another message is displayed. To update the firmware to the target level, update the firmware again. If event message indicates incompatible key, acquire the correct firmware version for a Chassis Management Module and retry the firmware update operation.

- **00015107 : Firmware update of [arg1] started by user ID [arg2] from [arg3] at IP address [arg4].**

The specified user has started a firmware update of the specified device.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information

Prefix: CMM **ID:** 0068

User Response
Information only; no action is required.

- **00015401 : System-management processor in [arg1] is in firmware update mode and must be updated.**

  The firmware in the specified node must be updated.

  Severity
  Informational

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0174

  User Response
  Update the update system firmware.

- **00015402 : System-management processor in [arg1] is in firmware update mode and must be updated.**

  The firmware in the specified node must be updated.

  Severity
  Informational

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0174

  User Response
  Update the update system firmware.

- **00015403 : System-management processor in [arg1] is in firmware update mode and must be updated.**

  The firmware in the specified node must be updated.

  Severity
  Informational

  Serviceable

Yes

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0174

User Response
Update the update system firmware.

- **00015404 : System-management processor in [arg1] is in firmware update mode and must be updated.**

  The firmware in the specified node must be updated.

  Severity
  Informational

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0174

  User Response
  Update the update system firmware.

- **00015405 : System-management processor in [arg1] is in firmware update mode and must be updated.**

  The firmware in the specified node must be updated.

  Severity
  Informational

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0174

User Response
Update the update system firmware.

- **00015406 : System-management processor in [arg1] is in firmware update mode and must be updated.**

  The firmware in the specified node must be updated.

  Severity
  Informational

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0174

  User Response
  Update the update system firmware.

- **00015407 : System-management processor in [arg1] is in firmware update mode and must be updated.**

  The firmware in the specified node must be updated.

  Severity
  Informational

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0174

  User Response
  Update the update system firmware.

- **00015408 : System-management processor in [arg1] is in firmware update mode and must be updated.**

  The firmware in the specified node must be updated.

  Severity
  Informational

  Serviceable
  Yes

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0174

User Response
Update the update system firmware.

- **00015409 : System-management processor in [arg1] is in firmware update mode and must be updated.**

  The firmware in the specified node must be updated.

  Severity
  Informational

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0174

  User Response
  Update the update system firmware.

- **0001540A : System-management processor in [arg1] is in firmware update mode and must be updated.**

  The firmware in the specified node must be updated.

  Severity
  Informational

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0174

  User Response
  Update the update system firmware.

- **0001540B : System-management processor in [arg1] is in firmware update mode and must be updated.**

  The firmware in the specified node must be updated.

  Severity
  Informational

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0174

  User Response
  Update the update system firmware.
- **0001540C : System-management processor in [arg1] is in firmware update mode and must be updated.**

  The firmware in the specified node must be updated.

  Severity
  Informational

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0174

  User Response
  Update the update system firmware.
- **0001540D : System-management processor in [arg1] is in firmware update mode and must be updated.**

  The firmware in the specified node must be updated.

  Severity
  Informational

  Serviceable
  Yes

  Automatically notify support
  No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0174

User Response
Update the update system firmware.

- **0001540E : System-management processor in [arg1] is in firmware update mode and must be updated.**

  The firmware in the specified node must be updated.

  Severity
  Informational

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0174

  User Response
  Update the update system firmware.

- **00015500 : Failed to change system-management processor management network interface [arg1] configuration of [arg2].**

  The external interface of the management network for the node cannot be set.

  Severity
  Informational

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0374

  User Response
  Complete the following steps until the problem is solved:

  1. Try to set the management network configuration for the node again.

2. Reset the system-management processor on the node.
3. Change the node settings, using the Setup utility.

- **00015503 : Chassis Management Module reset because of watchdog timeout.**

  The Chassis Management Module (CMM) has been reset because of a watchdog timeout. This CMM reset might be related to a change in the configuration of the CMM or the network.

  Severity
  Warning

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0557

  User Response
  Check the CMM event log to determine what changes have been made to the CMM that might have caused this event. If there are repeated failures in the log, contact Support.

- **00015504 : The operator is not permitted to change the power policy to consume more power than is available.**

  The power policy cannot be changed to a setting that enables the chassis to use more power than is available from a single power supply.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0637

  User Response
  Information only; no action is required.

- **00015505 : Wake on LAN for node in bay [arg1] was enabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has enabled Wake on LAN for the specified node.

  Severity
  Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0893

User Response
Information only; no action is required.

- **00015506 : Node [arg1] management network interface configuration updated by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has updated the node management network interface configuration.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0467

  User Response
  Information only; no action is required.

- **00015507 : Wake on LAN for all nodes was enabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has enabled wake on lan for all nodes.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0895

User Response
Information only; no action is required.

- **00015508 : Wake on LAN for node in bay [arg1] was disabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has disabled Wake on LAN for the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0894

  User Response
  Information only; no action is required.

- **00015509 : Wake on LAN for all nodes was disabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has disabled wake on lan for all nodes.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0896

  User Response
  Information only; no action is required.

- **00015510 : Chassis Management Module has securely erased user data.**

  The Chassis Management Module (CMM) user data has been securely erased. This includes any passwords, accounts, keys, or configurations on the system.

  Severity
  Warning

  Serviceable
  No

Automatically notify support
No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0809

User Response
Data on the Chassis Management Module (CMM) is cleared and is safe for disposal If there are repeated failures in the log, contact Support.

- **00015511 : Chassis Management Module was unable to securely erase user data.**

The Chassis Management Module (CMM) user data could not be securely erased.

Severity
Warning

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0810

User Response
Data on the Chassis Management Module (CMM) could not be erased securely. If there are repeated failures in the log, contact Support.

- **00015600 : Firmware update of standby Chassis Management Module from CMM [arg1] to CMM [arg2] was not completed ([arg3]).**

The firmware in the standby Chassis Management Module (CMM) is automatically updated if it is different from the firmware level in the primary CMM. The firmware update of the standby CMM has failed. The primary CMM and standby CMM are at different firmware levels.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information

Prefix: CMM **ID:** 0375

User Response
Update the primary CMM to the correct firmware level. The standby CMM will be updated automatically as a background operation.

- **00015700 : Firmware update of standby Chassis Management Module from CMM [arg1] to CMM [arg2] was completed.**

  The firmware update of the specified image from the primary Chassis Management Module (CMM) to the standby CMM was successful.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0376

  User Response
  Information only; no action is required.

- **00015800 : Management bus hang detected by both Chassis Management Modules.**

  Both Chassis Management Modules (CMMs) detected a communication problem on the I2C management bus. A device on the I2C bus might be unresponsive. The CMM will not failover again in an attempt to communicate with devices.

  Severity
  Warning

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0377

  User Response
  Solve errors in the Chassis Management Module event log pertaining to previous I2C messages that describe a specific problem.

- **00015803 : Chassis Management Module cannot convert the host name [arg1] to IP for syslog collector [arg2].**

  The Chassis Management Module (CMM) cannot resolve the specified host name for the specified syslog collector.

Severity
Informational

Serviceable
Yes

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0458

User Response
Complete the following steps until the problem is solved:

1. Make sure that the syslog collector is configured correctly and can be reached from the CMM.
2. Make sure that the Domain Name System (DNS) is configured correctly for host name resolution.

- **0001580B : Data collection for type [arg1] initiated for node [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has initiated data collection for the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0468

  User Response
  Information only; no action is required.

- **00015900 : Ethernet over USB interface for [arg1] was enabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has enabled the Ethernet over USB interface setting.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category

User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0905

User Response
Information only; no action is required.

- **00015902 : Node in bay [arg1] was requested to power off by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has powered off the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0943

  User Response
  Information only; no action is required.

- **00015903 : Node in bay [arg1] was requested to power on by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has powered on the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0944

  User Response
  Information only; no action is required.

- **00015904 : Power permission is not granted for this node. Power command was not sent to node [arg1].**

A power command has not been sent to a node because power permission has not been granted to that node. Power permission might not be granted if adequate power is not available for the node.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0634

User Response
Information only; no action is required.

- **00015905 : Power command sent to node [arg1] failed.**

The node has not accepted the power command. The node has responded with a Failed status or did not reply. Check for other messages, such as a communication problem or discovery.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0175

User Response
Information only; no action is required.

- **00015906 : The node in bay [arg1] was restarted by user ID [arg2] from [arg3] at IP address [arg4].**

The specified user has restarted the specified node.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0948

User Response
Information only; no action is required.

- **00015907 : The system-management processor in the node in bay [arg1] was restarted by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has restarted the system-management processor on the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0949

  User Response
  Information only; no action is required.

- **00015908 : Restoration of I/O module settings for bay [arg1] requested by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has reset the specified I/O module to the manufacturing default settings.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0588

  User Response
  Information only; no action is required.

- **00015B01 : Boot mode for node in node bay [arg1] set to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user set the boot mode to the new setting for the specified node. Boot mode typically allows the user to set the system to boot from temporary or permanent side of the firmware bank.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0743

User Response
Information only; no action is required.

- **00015B02 : Boot mode for node in node bay [arg1] set to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user set the boot mode to the new setting for the specified node. Boot mode typically allows the user to set the system to boot from temporary or permanent side of the firmware bank.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0743

  User Response
  Information only; no action is required.

- **00015B03 : Boot mode for node in node bay [arg1] set to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user set the boot mode to the new setting for the specified node. Boot mode typically allows the user to set the system to boot from temporary or permanent side of the firmware bank.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0743

User Response
Information only; no action is required.

- **00015B04 : Boot mode for node in node bay [arg1] set to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user set the boot mode to the new setting for the specified node. Boot mode typically allows the user to set the system to boot from temporary or permanent side of the firmware bank.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0743

  User Response
  Information only; no action is required.

- **00015B05 : Boot mode for node in node bay [arg1] set to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user set the boot mode to the new setting for the specified node. Boot mode typically allows the user to set the system to boot from temporary or permanent side of the firmware bank.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0743

  User Response
  Information only; no action is required.

- **00015B06 : Boot mode for node in node bay [arg1] set to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

The specified user set the boot mode to the new setting for the specified node. Boot mode typically allows the user to set the system to boot from temporary or permanent side of the firmware bank.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0743

User Response
Information only; no action is required.

- **00015B07 : Boot mode for node in node bay [arg1] set to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user set the boot mode to the new setting for the specified node. Boot mode typically allows the user to set the system to boot from temporary or permanent side of the firmware bank.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0743

  User Response
  Information only; no action is required.

- **00015B08 : Boot mode for node in node bay [arg1] set to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user set the boot mode to the new setting for the specified node. Boot mode typically allows the user to set the system to boot from temporary or permanent side of the firmware bank.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0743

User Response
Information only; no action is required.

- **00015B09 : Boot mode for node in node bay [arg1] set to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user set the boot mode to the new setting for the specified node. Boot mode typically allows the user to set the system to boot from temporary or permanent side of the firmware bank.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0743

  User Response
  Information only; no action is required.

- **00015B0A : Boot mode for node in node bay [arg1] set to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user set the boot mode to the new setting for the specified node. Boot mode typically allows the user to set the system to boot from temporary or permanent side of the firmware bank.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0743

  User Response
  Information only; no action is required.

- **00015B0B : Boot mode for node in node bay [arg1] set to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user set the boot mode to the new setting for the specified node. Boot mode typically allows the user to set the system to boot from temporary or permanent side of the firmware bank.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0743

  User Response
  Information only; no action is required.
- **00015B0C : Boot mode for node in node bay [arg1] set to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user set the boot mode to the new setting for the specified node. Boot mode typically allows the user to set the system to boot from temporary or permanent side of the firmware bank.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0743

  User Response
  Information only; no action is required.
- **00015B0D : Boot mode for node in node bay [arg1] set to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user set the boot mode to the new setting for the specified node. Boot mode typically allows the user to set the system to boot from temporary or permanent side of the firmware bank.

  Severity
  Informational

  Serviceable
  No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0743

User Response
Information only; no action is required.

- **00015B0E : Boot mode for node in node bay [arg1] set to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user set the boot mode to the new setting for the specified node. Boot mode typically allows the user to set the system to boot from temporary or permanent side of the firmware bank.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0743

  User Response
  Information only; no action is required.

- **00015C01 : Boot Sequence for node in node bay [arg1] has changed by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user changed the boot sequence for the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0760

  User Response

Information only; no action is required.

- **00016001 : Chassis Management Module network initialization complete.**

  The network initialization of the primary Chassis Management Module is complete.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0011

  User Response
  Information only; no action is required.

- **0001600B : The [arg1] log has been cleared by user ID [arg2] from [arg3] at address [arg4].**

  The Chassis Management Module log specified in [arg1] has been cleared. The specified log can be "system" or "audit".

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0004

  User Response
  Information only; no action is required.

- **0001600D : Do not log new authentication events for the same user for, changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the specified duration for the "Do not log new authentication events for the same user for" setting.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support

No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0138

User Response
Information only; no action is required.

- **0001600E : The setting, Ignore client IP address when tracking user authentication events, was changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the "Ignore client IP address when tracking user authentication events" setting.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0139

  User Response
  Information only; no action is required.

- **0001600F : Certificate error for [arg1]. Additional information: [arg2].**

  Trusted certificates are imported to the Chassis Management Module (CMM) and used by the CMM Secure Sockets Layer (SSL) client to authenticate the user to the server SSL certificate. The CMM has detected that trusted certificate 1 is not valid.

  Severity
  Warning

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0622

  User Response

Delete or reinstall the trusted certificate.

- **00016010 : Certificate error for [arg1]. Additional information: [arg2].**

  Trusted certificates are imported to the Chassis Management Module (CMM) and used by the CMM Secure Sockets Layer (SSL) client to authenticate the user to the server SSL certificate. The CMM has detected that trusted certificate 1 is not valid.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0622

  User Response
  Delete or reinstall the trusted certificate.

- **00016011 : Certificate error for [arg1]. Additional information: [arg2].**

  Trusted certificates are imported to the Chassis Management Module (CMM) and used by the CMM Secure Sockets Layer (SSL) client to authenticate the user to the server SSL certificate. The CMM has detected that trusted certificate 1 is not valid.

  Severity
  Warning

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0622

  User Response
  Delete or reinstall the trusted certificate.

- **00016012 : Certificate error for [arg1]. Additional information: [arg2].**

  Trusted certificates are imported to the Chassis Management Module (CMM) and used by the CMM Secure Sockets Layer (SSL) client to authenticate the user to the server SSL certificate. The CMM has detected that trusted certificate 1 is not valid.

  Severity
  Warning

  Serviceable

No

Automatically notify support
No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0622

User Response
Delete or reinstall the trusted certificate.

- **00016013 : Certificate error for [arg1]. Additional information: [arg2].**

  Trusted certificates are imported to the Chassis Management Module (CMM) and used by the CMM Secure Sockets Layer (SSL) client to authenticate the user to the server SSL certificate. The CMM has detected that trusted certificate 1 is not valid.

  Severity
  Warning

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0622

  User Response
  Delete or reinstall the trusted certificate.

- **00016014 : Standby Chassis Management Module [arg1] certificate error. Additional information: [arg2].**

  Trusted certificates are imported to the Chassis Management Module (CMM) and used by the Secure Sockets Layer (SSL) client to authenticate the LDAP server SSL certificate. The CMM has detected that the specified trusted certificate is not valid.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0624

User Response
Reinstall the trusted certificate.

- **00016015 : IPv4 address of primary Chassis Management Module is the same as the IPv4 address of standby Chassis Management Module. Standby network interface is disabled.**

  The IP address of primary Chassis Management Module (CMM) is the same as the IP address of the standby CMM. The network interface of the standby CMM has been disabled.

  Severity
  Warning

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0146

  User Response
  Assign a different IP address to the standby Chassis Management Module.

- **00016016 : User account is active: [arg1].**

  The specified user has changed the specified login profile (user account) to Active state. The user can now access the Chassis Management Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0454

  User Response
  Information only; no action is required.

- **00016017 : Account has been inactive for more than the configured inactivity alert limit for user [arg1].**

  The specified login profile (user account) is dormant because the user has not attempted to log in to the Chassis Management Module (CMM) for a specified period of time (inactivity alert period).

  Severity

Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0455

User Response
If the specified user account needs continued access to the CMM, use one of the following procedures:
- Notify the owner of the user account to log in to the CMM. This will reset the login profile to Active state.
- Reset the login profile to Active state. You must have supervisor or chassis configuration authority to reset the login profile of the user account.

- **00016018 : Account has been disabled because of inactivity for more than the configured limit for user [arg1].**

The specified login profile (user account) has been disabled because of inactivity.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0456

User Response
If the specified user account needs continued access to the Chassis Management Module, reset the login profile to Active state. You must have supervisor or chassis configuration authority to reset the login profile of the user account.

- **00016019 : Account has been inactive for longer than the configured disable and alert limit for supervisor [arg1].**

The amount of time that the supervisor account has been inactive exceeds the configured alert and disable limits.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0230

User Response
If this user account is still required, the owner of the user account must log in to the Chassis Management Module.

- **0001601A : Logoff successful. User ID [arg1] from [arg2] at IP address [arg3].**

The specified user has logged out of the Chassis Management Module.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0002

User Response
Information only; no action is required.

- **0001601B : The [arg1] log has been cleared by user ID [arg2] from [arg3] at address [arg4].**

The Chassis Management Module log specified in [arg1] has been cleared. The specified log can be "system" or "audit".

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0004

User Response
Information only; no action is required.

- **0001601C : CMM moved from [arg1] to [arg2]. Clearing logs from previous chassis.**

  The Chassis Management Module (CMM) event logs that were recorded on a previous chassis were removed because the CMM was moved to a new chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0644

  User Response
  Information only; no action is required.
- **0001601D : Cryptographic compliance mode change to [arg1] was initiated by user ID [arg2] from [arg3] at IP address [arg4].**

  A change of the active cryptographic compliance mode was initiated by the specified user ID.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0744

  User Response
  Information only.
- **0001601E : Cryptographic compliance mode change to [arg1] was completed.**

  A change of the active cryptographic compliance mode was completed.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category

Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0745

User Response
Information only.

- **0001601F : Cipher Suites List Selection Was Changed To [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  A selection of TLS version specific cipher suites was completed by the specified user ID.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0693

  User Response
  Information only; See document "CMM TLS Version Select Cipher Suite" help to understand the benefits and limits of the two available choices [Legacy, Restricted].

- **00016020 : Account password will expire for user [arg1] in [arg2] days.**

  The password for the specified user account will expire within 7 days.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0231

  User Response
  The owner of the user account must change the password.

- **00016021 : Account security level changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the account security level for the specified user account.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0537

User Response
Information only; no action is required.

- **00016022 : Maximum number of login failures setting changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the "Maximum number of login failures" account security setting.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0538

  User Response
  Information only; no action is required.

- **00016023 : Password expiration period setting changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the password expiration time interval (the amount of time that a password is valid before it expires). This setting determines the amount of time that a password is in effect before it automatically expires.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0539

User Response
Information only; no action is required.

- **00016024 : Default account password must be changed on next login setting was enabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has enabled the "Factory default 'USERID' account password must be changed on next login" setting. This setting determines that the USERID account must change the password the next time the password is used to log in to the Chassis Management Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0980

  User Response
  Information only; no action is required.

- **00016025 : Minimum password reuse cycle setting changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the "Minimum password reuse cycle" setting. This setting determines how often you can reuse a previously used password.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0541

  User Response
  Information only; no action is required.

- **00016026 : Complex password rules setting was enabled by user ID [arg1] from [arg2] at IP address [arg3].**

The specified user has enabled the "Complex password rules" setting. This setting determines the type of password that is acceptable.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0982

User Response
Information only; no action is required.

- **00016027 : Minimum different characters in passwords setting changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the "Minimum different characters in passwords" setting. This setting determines how many unique characters must be used when a password is created or changed.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0543

  User Response
  Information only; no action is required.

- **00016028 : Force user to change password on first login setting was enabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has enabled the "Force user to change password on first access" setting. The user must change the password the next time the user logs in to the Chassis Management Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0984

User Response
Information only; no action is required.

- **00016029 : Inactivity alert period setting changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the "Inactivity alert period" setting. This setting determines how long a user account can be inactive (not used to log in) before it becomes dormant.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0545

  User Response
  Information only; no action is required.

- **0001602A : Inactivity alert and disable period setting changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the "Inactivity alert and disable period" setting. This setting determines how long a user account can be inactive (not used to log in) before it is disabled. An alert will be generated before a user account is disabled.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0546

  User Response

Information only; no action is required.

- **0001602B : Lockout period after maximum login failures setting changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the "Lockout period after maximum login failures" setting. This setting determines the length of time that a user account is locked out after the maximum number of login failures is exceeded.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0547

  User Response
  Information only; no action is required.

- **0001602C : User login password required setting changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the "User login password required" setting. This setting determines whether a password is required when a user logs in to the Chassis Management Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0548

  User Response
  Information only; no action is required.

- **0001602D : Account disabled for user [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has disabled the specified user account.

  Severity
  Informational

  Serviceable
  No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0136

User Response
Information only; no action is required.

- **0001602E : Account enabled for user [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has enabled the specified user account.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0135

  User Response
  Information only; no action is required.

- **0001602F : Account unlocked for user [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user account has been unlocked.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0137

  User Response
  Information only; no action is required.

- **00016030 : LDAP authentication method changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

The specified user has changed the "User authentication method" setting. This setting determines how users are authenticated when they log in.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0450

User Response
Information only; no action is required.

- **00016031 : Web inactivity timeout changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the "Inactive session timeout value" setting. This setting determines how long a user interface session can remain idle before the session times out.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0451

  User Response
  Information only; no action is required.

- **00016032 : Telnet inactivity timeout changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the "command-line session timeout" setting. This setting determines how long a command-line session can be idle before the session times out.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0452

User Response
Information only; no action is required.

- **00016033 : HTTP port number changed from [arg1] to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The HTTP port number has been changed. New HTTP (web) connections must use the new port number.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0077

  User Response
  Information only; no action is required.

- **00016034 : HTTPS port number changed from [arg1] to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The HTTPS port number has been changed. New HTTPS (secure web) connections must use the new port number.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0078

  User Response
  Information only; no action is required.

- **00016035 : Telnet port number changed from [arg1] to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The Telnet port number has been changed.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0079

  User Response
  Information only; no action is required.
- **00016036 : SSH port number changed from [arg1] to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The Secure Shell (SSH) port number has been changed.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0080

  User Response
  Information only; no action is required.
- **00016037 : SNMP agent port number changed from [arg1] to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The Simple Network Management Protocol (SNMP) agent port number has been changed.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0081

User Response
Information only; no action is required.

- **00016038 : SNMP traps port number changed from [arg1] to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the Simple Network Management Protocol (SNMP) traps port number.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0082

  User Response
  Information only; no action is required.

- **00016039 : TCP Command mode port number changed from [arg1] to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The Transmission Control Protocol (TCP) Command mode port number has been changed.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0083

  User Response
  Information only; no action is required.

- **0001603A : Secure TCP Command mode port number changed from [arg1] to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

The Secure Transmission Control Protocol Command mode port number has been changed.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0084

User Response
Information only; no action is required.

- **0001603B : FTP port number changed from [arg1] to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The File Transfer Protocol (FTP) port number has been changed.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0085

  User Response
  Information only; no action is required.

- **0001603C : FTP data port number changed from [arg1] to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The File Transfer Protocol (FTP) data port number has been changed.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0086

User Response
Information only; no action is required.

- **0001603D : TFTP port number changed from [arg1] to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The Trivial File Transfer Protocol (TFTP) port number has been changed.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0087

  User Response
  Information only; no action is required.

- **0001603E : SFTP port number changed from [arg1] to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The Simple File Transfer Protocol (SFTP) port number has been changed.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0088

  User Response
  Information only; no action is required.

- **00016044 : SLP port number changed from [arg1] to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The Service Location Protocol (SLP) port number has been changed.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0089

User Response
Information only; no action is required.

- **00016048 : SLP service was enabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has enabled The Service Location Protocol (SLP) service.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0917

  User Response
  Information only; no action is required.

- **00016049 : Web server port was enabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has enabled the Web server port.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information

Prefix: CMM **ID:** 0919

User Response
Information only; no action is required.

- **0001604A : IP port numbers reset to defaults by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has reset all network port numbers to their default values. Changes will take effect when the Chassis Management Module is restarted.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0472

  User Response
  Information only; no action is required.

- **0001604B : TCP Command mode port numbers reset to defaults by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has reset the Transmission Control Protocol (TCP) Command mode port number to its default value. Changes will take effect when the Chassis Management Module is restarted.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0473

  User Response
  Information only; no action is required.

- **0001604E : Password encryption [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  Data encryption has been changed. If it is enabled, user passwords are stored in NVRAM in encrypted format. Otherwise, passwords are stored in plain text.

  Severity
  Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0218

User Response
Information only; no action is required.

- **0001604F : The account for user ID [arg1] was deleted by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has deleted the specified user account.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0134

  User Response
  Information only; no action is required.

- **00016050 : The password expired for user [arg1].**

  The password for the specified user account has expired.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0234

User Response
Change the password for the specified user account.

- **00016051 : A password is required for user [arg1].**

  A password is required for the specified user account.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0140

  User Response
  Information only; no action is required.

- **00016053 : Serial port baud rate changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the baud rate of the Chassis Management Module serial port.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0501

  User Response
  Information only; no action is required.

- **00016054 : Serial port parity changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the parity setting of the serial port has been changed.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0502

User Response
Information only; no action is required.

- **00016055 : Serial port stop bits setting changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the stop bits setting of the serial port has been changed.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0503

  User Response
  Information only; no action is required.

- **00016057 : Telnet service was enabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has enabled Telnet.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0881

  User Response
  Information only; no action is required.

- **00016058 : FTP server was enabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has enabled File Transfer Protocol (FTP).

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0909

User Response
Information only; no action is required.

- **00016059 : TFTP server was enabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has enabled Trivial File Transfer Protocol (TFTP).

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0911

  User Response
  Information only; no action is required.

- **0001605A : SFTP server was enabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has enabled Secure File Transfer Protocol (SFTP).

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information

Prefix: CMM **ID:** 0913

User Response
Information only; no action is required.

- **0001605B : NTP server was enabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has enabled Network Time Protocol (NTP).

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0915

  User Response
  Information only; no action is required.

- **0001605C : FTP timeout changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the File Transfer Protocol (FTP) timeout. This setting determines the amount of time that an FTP connection can be inactive before it is closed.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0474

  User Response
  Information only; no action is required.

- **0001605D : (Secure) TCP Command mode inactivity timeout changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the Transmission Control Protocol (TCP) command-mode timeout. This setting determines the amount of time that a TCP command-mode connection can be inactive before it is closed.

  Severity
  Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0475

User Response
Information only; no action is required.

- **0001605E : TCP Command mode changed from [arg1] to [arg2] connection(s) by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the maximum number of user connections for TCP Command mode.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0210

  User Response
  Information only; no action is required.

- **0001605F : SNMP traps disabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has disabled Simple Network Management Protocol (SNMP) traps.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0888

User Response
Information only; no action is required.

- **00016060 : SNMP v1 was enabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has enabled the SNMPv1 agent.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0883

  User Response
  Information only; no action is required.

- **00016061 : SNMPv1 community configuration changed by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has changed the SNMPv1 community configuration.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0476

  User Response
  Information only; no action is required.

- **00016062 : The configuration of alert recipient [arg1] was deleted by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has deleted the configuration of the specified remote alert recipient.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support

No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0706

User Response
Information only; no action is required.

- **00016063 : The name of alert recipient [arg1] was changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the name of the specified remote alert recipient.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0707

  User Response
  Information only; no action is required.

- **00016064 : The status of alert recipient [arg1] was changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the status of the specified remote alert recipient.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0708

  User Response
  Information only; no action is required.

- **00016065 : The filter of alert recipient [arg1] was changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the filter of the specified remote alert recipient.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0709

  User Response
  Information only; no action is required.
- **00016066 : The type of alert recipient [arg1] was changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the type of the specified remote alert recipient.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0710

  User Response
  Information only; no action is required.
- **00016067 : The email adress of alert recipient [arg1] was changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the email of the specified remote alert recipient.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0711

User Response
Information only; no action is required.

- **00016068 : The date and time were changed by user ID [arg1] from [arg2] at IP address [arg3].**

The specified user has changed the date and time in the Chassis Management Module.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0561

User Response
Information only; no action is required.

- **00016069 : The time zone was changed by user ID [arg1] from [arg2] at IP address [arg3].**

The specified user has changed the time zone.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0562

User Response
Information only; no action is required.

- **0001606A : Daylight saving time setting changed by user ID [arg1] from [arg2] at IP address [arg3].**

The specified user has changed the daylight saving time setting.

Severity

Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0629

User Response
Information only; no action is required.

- **0001606B : SSH protocol was disabled by user ID [arg1] from [arg2] at IP address [arg3].**

  A user has disabled the Secure Shell (SSH) service.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0904

  User Response
  Information only; no action is required.

- **0001606C : SSH protocol was enabled by user ID [arg1] from [arg2] at IP address [arg3].**

  A user has enabled the Secure Shell (SSH) service.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0903

User Response
Information only; no action is required.

- **0001606E : SSH host key manual generation completed.**

  The Secure Shell (SSH) host key has been created.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0202

  User Response
  Information only; no action is required.

- **0001606F : Minimum password change interval setting changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the minimum password change interval. This change applies to all local users.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0549

  User Response
  Information only; no action is required.

- **00016070 : SNMP community configuration changed by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has changed the Simple Network Management Protocol (SNMP) configuration.

  Severity
  Informational

  Serviceable
  No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0477

User Response
Information only; no action is required.

- **00016071 : DNS configuration changed by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has changed the Domain Name System (DNS) configuration.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0478

  User Response
  Information only; no action is required.

- **00016072 : SMTP server address changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the Simple Mail Transfer Protocol (SMTP) configuration.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0479

  User Response
  Information only; no action is required.

- **00016073 : The LDAP configuration was changed by user ID [arg1] from [arg2] at IP address [arg3].**

The specified user has changed the Lightweight Directory Access Protocol (LDAP) configuration.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0148

User Response
Information only; no action is required.

- **00016074 : Trespass message has been [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

The trespass warning message has been enabled or disabled.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0258

User Response
Information only; no action is required.

- **00016075 : Trespass warning message changed by user ID [arg1] from [arg2] at IP address [arg3].**

The specified user has changed the trespass warning message.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0156

User Response
Information only; no action is required.

- **00016076 : Account has been disabled for user [arg1].**

The specified user account has been disabled.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0232

User Response
Information only; no action is required.

- **00016077 : Account created for user [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

The specified user has created the specified user account.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0133

User Response
Information only; no action is required.

- **00016079 : NTP server host updated to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

The specified user has changed the Network Time Protocol (NTP) server host name or IP address.

Severity
Informational

Serviceable
No

Automatically notify support

No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0558

User Response
Information only; no action is required.

- **0001607A : NTP update frequency changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the Network Time Protocol (NTP) update frequency.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0559

  User Response
  Information only; no action is required.

- **0001607B : NTPv3 authentication was enabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has enabled the Network Time Protocol (NTP) v3 authentication.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0921

  User Response
  Information only; no action is required.

- **0001607C : NTPv3 authentication settings changed by user ID [arg1] from [arg2] at IP address [arg3].**

The specified user has changed the Network Time Protocol (NTP) v3 authentication settings.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0560

User Response
Information only; no action is required.

- **0001607D : Password changed for user [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the password for the specified user account.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0235

  User Response
  Information only; no action is required.

- **0001607E : The access rights changed for user [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the user authority level for the specified user account.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID

mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0453

User Response
Information only; no action is required.

- **0001607F : The configuration of alert recipient [arg1] was modified by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the configuration of the specified remote alert recipient.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0705

  User Response
  Information only; no action is required.

- **00016081 : Syslog collector 1 was enabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has enabled syslog collector 1.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0874

  User Response
  Information only; no action is required.

- **00016082 : Syslog collector 2 was enabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has enabled syslog collector 2.

  Severity
  Informational

  Serviceable

No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0875

User Response
Information only; no action is required.

- **00016083 : Host name of syslog collector 1 has been changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the host name or IP address that is used for syslog collector 1.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0504

  User Response
  Information only; no action is required.

- **00016084 : Host name of syslog collector 2 has been changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the host name or IP address that is used for syslog collector 2.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0505

User Response
Information only; no action is required.

- **00016085 : Port number of syslog collector 1 has been changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the port number that is used for syslog collector 1.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0506

  User Response
  Information only; no action is required.

- **00016086 : Port number of syslog collector 2 has been changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the port number that is used for syslog collector 2.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0507

  User Response
  Information only; no action is required.

- **00016087 : SSH public key deleted by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has deleted the Secure Shell (SSH) public key.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support

No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0203

User Response
Information only; no action is required.

- **00016088 : SSH public key modified by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has modified the Secure Shell (SSH) public key.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0204

  User Response
  Information only; no action is required.

- **00016089 : SSH public key installed by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has installed the Secure Shell (SSH) public key.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0205

  User Response
  Information only; no action is required.

- **0001608A : SSH host key manual generation started by user ID [arg1] from [arg2] at IP address [arg3].**

The specified user is manually creating a Secure Shell (SSH) host key.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0201

User Response
Information only; no action is required.

- **0001608B : SSH host key manual generation failed.**

The Secure Shell (SSH) host key has not been created.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0206

User Response
Regenerate the host key.

- **0001608C : SSH host key auto-generation started.**

The Secure Shell (SSH) host key auto-generation process has started. This message might be displayed after you restore the default configuration of the Chassis Management Module.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID

mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0207

User Response
Information only; no action is required.

- **0001608D : SSH host key auto-generation completed.**

The Secure Shell (SSH) host key auto-generation is complete.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0208

User Response
Information only; no action is required.

- **0001608E : SSH host key auto-generation failed.**

Secure Shell (SSH) host key auto-generation has failed.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0209

User Response
Regenerate the host key.

- **0001608F : [arg1] alert recipient [arg2] was created by user ID [arg3] from [arg4] at IP address [arg5]. Its status is [arg6]. Its filter is [arg7].**

The specified user has created the configuration of the specified remote alert recipient.

Severity
Informational

Serviceable

No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0712

User Response
Information only; no action is required.

- **00016090 : Maximum concurrent active sessions for user acount [arg1] set to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has set the maximum concurrent active sessions for local users.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0151

  User Response
  Information only; no action is required.

- **00016091 : Maximum concurrent active sessions for LDAP login profile set to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has set the maximum concurrent active sessions for the specified LDAP login profile.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0152

User Response
Information only; no action is required.

- **00016093 : Session for user [arg1] terminated.**

  The specified user has terminated the specified user session.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0154

  User Response
  Information only; no action is required.

- **00016097 : Local power control for node in bay [arg1] was enabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has enabled local power control for the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0897

  User Response
  Information only; no action is required.

- **00016098 : Local power control for all nodes was enabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has enabled local power control for all nodes.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support

No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0899

User Response
Information only; no action is required.

- **00016099 : SSL server was enabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has enabled the Secure Sockets Layer (SSL) server.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0930

  User Response
  Information only; no action is required.

- **0001609A : SSL client was enabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has enabled the Secure Sockets Layer (SSL) client.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0932

  User Response
  Information only; no action is required.

- **0001609B : Standby Chassis Management Module SSL server [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

The specified user has enabled or disabled the Secure Sockets Layer (SSL) server on the standby Chassis Management Module.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0223

User Response
Information only; no action is required.

- **0001609C : Certificate deleted for [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

The specified user has deleted Secure Sockets Layer (SSL) trusted client certificate number 1.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0613

User Response
Information only; no action is required.

- **0001609E : Certificate deleted for [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

The specified user has deleted Secure Sockets Layer (SSL) trusted client certificate number 1.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID

mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0613

User Response
Information only; no action is required.

- **000160A0 : Standby Chassis Management Module [arg1] certificate deleted by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has deleted the Secure Sockets Layer (SSL) server certificate on the standby Chassis Management Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0617

  User Response
  Information only; no action is required.

- **000160A2 : Certificate imported for [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has imported a Certificate Authority signed certificate.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0626

  User Response
  Information only; no action is required.

- **000160A3 : Certificate imported for [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has imported a Certificate Authority signed certificate.

  Severity
  Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0626

User Response
Information only; no action is required.

- **000160A4 : Standby Chassis Management Module [arg1] certificate imported by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has imported a Certificate Authority signed certificate on the standby Chassis Management Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0627

  User Response
  Information only; no action is required.

- **000160A5 : Self-signed certificate for [arg1] created by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has created a self-signed certificate.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information

Prefix: CMM **ID:** 0612

User Response
Information only; no action is required.

- **000160A6 : Self-signed certificate for [arg1] created by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has created a self-signed certificate.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0612

  User Response
  Information only; no action is required.

- **000160A7 : Self-signed certificate created for [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has imported a Certificate Authority signed Secure Sockets Layer (SSL) server certificate on the standby Chassis Management Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0616

  User Response
  Information only; no action is required.

- **000160AB : Secure TCP Command mode changed from [arg1] to [arg2] connection(s) by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has enabled or disabled Secure TCP Command mode.

  Severity
  Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0851

User Response
Information only; no action is required.

- **000160AC : Test syslog generated by user ID [arg1] from [arg2] at IP address [arg3].**

The specified user has generated a syslog test event.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0379

User Response
If the syslog collector received the test event, no action is required. If the syslog collector did not receive the test event, complete the following steps until the problem is solved:

1. Make sure that the syslog collector is configured correctly and is running.
2. Make sure that the syslog collector can be reached from the CMM.

- **000160AD : Certificate signing request created for [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

The specified user has created a certificate signing request.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID

mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0614

User Response
Information only; no action is required.

- **000160AE : Certificate signing request deleted for [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has deleted a certificate signing request.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0615

  User Response
  Information only; no action is required.

- **000160AF : Certificate signing request created for [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has created a certificate signing request.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0614

  User Response
  Information only; no action is required.

- **000160B0 : Certificate signing request deleted for [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has deleted a certificate signing request.

  Severity

Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0615

User Response
Information only; no action is required.

- **000160B1 : Standby Chassis Management Module [arg1] certificate signing request created by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has created a certificate signing request on the standby Chassis Management Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0618

  User Response
  Information only; no action is required.

- **000160B2 : Standby Chassis Management Module [arg1] certificate signing request deleted by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has deleted a certificate signing request on the standby Chassis Management Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0619

User Response
Information only; no action is required.

- **000160B3 : Certificate imported for [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

The specified user has imported a certificate.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0620

User Response
Information only; no action is required.

- **000160B4 : Certificate deleted for [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

The specified user has deleted Secure Sockets Layer (SSL) trusted client certificate number 1.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0613

User Response
Information only; no action is required.

- **000160B5 : Certificate imported for [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

The specified user has imported a certificate.

Severity
Informational

Serviceable
No

Automatically notify support

No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0620

User Response
Information only; no action is required.

- **000160B6 : Certificate deleted for [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has deleted Secure Sockets Layer (SSL) trusted client certificate number 1.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0613

  User Response
  Information only; no action is required.

- **000160B7 : Certificate imported for [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has imported a certificate.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0620

  User Response
  Information only; no action is required.

- **000160B8 : Certificate deleted for [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has deleted Secure Sockets Layer (SSL) trusted client certificate number 1.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0613

User Response
Information only; no action is required.

- **000160BA : The date and time were changed by [arg1] days [arg2] hours [arg3] minutes [arg4] seconds by user ID [arg5] from [arg6] at IP address [arg7].**

  The specified user has changed the date and time in the Chassis Management Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0648

  User Response
  Information only; no action is required.

- **000160BB : The time zone was changed from [arg1] to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the time zone.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0649

User Response
Information only; no action is required.

- **000160BC : The NTP server adjusted the Chassis Management Module clock by [arg1] days [arg2] hours [arg3] minutes [arg4] seconds.**

  NTP has adjusted the time in the Chassis Management Module by more than 2 minutes.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0650

  User Response
  Information only; no action is required.

- **000160BD : SSL setting for the external LDAP client changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  SSL setting for the external LDAP client changed to the specified value by the specified user.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0793

  User Response
  Information only; no action is required.

- **000160BE : Local power control for node in bay [arg1] was disabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has disabled local power control for the specified node.

  Severity
  Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0898

User Response
Information only; no action is required.

- **000160BF : Local power control for all nodes was disabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has disabled local power control for all nodes.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0900

  User Response
  Information only; no action is required.

- **000160C0 : Group [arg1] created by user ID [arg2] from [arg3] at IP address [arg4].**

  Group specified created by the specified user account.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0228

User Response
Information only; no action is required.

- **000160C1 : Group name [arg1] changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  Group name specified changed to specified by the specified user account.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0229

  User Response
  Information only; no action is required.

- **000160C2 : Permission for group [arg1] were changed by user ID [arg2] from [arg3] at IP address [arg4].**

  Permission for group specified were changed by specified user.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0178

  User Response
  Information only; no action is required.

- **000160C3 : Group [arg1] deleted by user ID [arg2] from [arg3] at IP address [arg4].**

  Group specified deleted by the specified user account.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0194

User Response
Information only; no action is required.

- **000160C4 : Account role [arg1] created by user ID [arg2] from [arg3] at IP address [arg4].**

  Account role specified created by the specified user account.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0283

  User Response
  Information only; no action is required.

- **000160C5 : Account role [arg1] changed by user ID [arg2] from [arg3] at IP address [arg4].**

  Account role specified changed by the specified user account.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0284

  User Response
  Information only; no action is required.

- **000160C6 : Account role [arg1] deleted by user ID [arg2] from [arg3] at IP address [arg4].**

  Account role specified deleted by the specified user account.

  Severity

Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0285

User Response
Information only; no action is required.

- **000160C7 : DNS SRV domain source changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  DNS SRV domain source changed to specified by the specified user account.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0286

  User Response
  Information only; no action is required.

- **000160C8 : DNS SRV service source changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  DNS SRV service source changed to specified by the specified user account.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0287

User Response
Information only; no action is required.

- **000160C9 : Authentication Only mode was set to [arg1] (enabled) by user ID [arg2] from [arg3] at IP address [arg4].**

  LDAP Authentication Only mode was enabled by the specified user account.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0288

  User Response
  Information only; no action is required.

- **000160CA : Authentication Only mode was set to [arg1] (disabled) by user ID [arg2] from [arg3] at IP address [arg4].**

  LDAP Authentication Only mode was disabled by the specified user account.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0289

  User Response
  Information only; no action is required.

- **000160CB : LDAP forest name changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  LDAP forest name changed to specified by the specified user account.

  Severity
  Informational

  Serviceable

No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0328

User Response
Information only; no action is required.

- **000160CC : Group profile ID [arg1] renamed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified group profile ID was renamed to the indicated group profile ID by the specified user account.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0695

  User Response
  Information only; no action is required.

- **000160CD : Account role [arg1] renamed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user renamed the specified account role.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0761

User Response
Information only; no action is required.

- **000160CE : NTPv3 authentication was disabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has disabled the Network Time Protocol (NTP) v3 authentication.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0922

  User Response
  Information only; no action is required.

- **000160D0 : SNMP v3 was enabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has enabled SNMPv3 agent.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0885

  User Response
  Information only; no action is required.

- **000160D1 : Syslog collector 1 was disabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has disabled syslog collector 1.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category

User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0876

User Response
Information only; no action is required.

- **000160D2 : Syslog collector 2 was disabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has disabled syslog collector 2.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0877

  User Response
  Information only; no action is required.

- **000160D3 : Syslog filtering level was changed to error by user ID [arg1] from [arg2] at IP address [arg3].**

  The severity filtering level has been changed to error for the syslog protocol. Only events with severity error will be send.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0878

  User Response
  Information only; no action is required.

- **000160D4 : Syslog filtering level was changed to warning by user ID [arg1] from [arg2] at IP address [arg3].**

The severity filtering level has been changed to warning for the syslog protocol. Events with severity warning and error will be send.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0879

User Response
Information only; no action is required.

- **000160D5 : Syslog filtering level was changed to informational by user ID [arg1] from [arg2] at IP address [arg3].**

The severity filtering level has been changed to informational for the syslog protocol. Events with severity informational, warning and error will be send.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0880

User Response
Information only; no action is required.

- **000160D6 : Telnet service was disabled by user ID [arg1] from [arg2] at IP address [arg3].**

The specified user has disabled Telnet.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category

User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0882

User Response
Information only; no action is required.

- **000160D7 : SNMP v1 was disabled by user ID [arg1] from [arg2] at IP address [arg3].**

The specified user has disabled SNMPv1 agent.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0884

User Response
Information only; no action is required.

- **000160D8 : SNMP v3 was disabled by user ID [arg1] from [arg2] at IP address [arg3].**

The specified user has disabled SNMPv3 agent.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0886

User Response
Information only; no action is required.

- **000160D9 : SNMP traps enabled by user ID [arg1] from [arg2] at IP address [arg3].**

The specified user has enabled Simple Network Management Protocol (SNMP) traps.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0887

User Response
Information only; no action is required.

- **000160DA : Ethernet over USB interface for [arg1] was disabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has disabled the Ethernet over USB interface setting.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0906

  User Response
  Information only; no action is required.

- **000160DB : FTP server was disabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has disabled File Transfer Protocol (FTP).

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0910

User Response
Information only; no action is required.

- **000160DC : TFTP server was disabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has disabled Trivial File Transfer Protocol (TFTP).

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0912

  User Response
  Information only; no action is required.

- **000160DD : SFTP server was disabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has disabled Secure File Transfer Protocol (SFTP).

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0914

  User Response
  Information only; no action is required.

- **000160DE : NTP server was disabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has disabled Network Time Protocol (NTP).

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category

User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0916

User Response
Information only; no action is required.

- **000160DF : SLP service was disabled by user ID [arg1] from [arg2] at IP address [arg3].**

The specified user has disabled The Service Location Protocol (SLP) service.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0918

User Response
Information only; no action is required.

- **000160E0 : Web session has timed out for user [arg1].**

Web session has timed out for the specified user.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0746

User Response
Information only; no action is required.

- **000160E1 : Web server port was disabled by user ID [arg1] from [arg2] at IP address [arg3].**

The specified user has disabled the Web server port.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0920

User Response
Information only; no action is required.

- **000160F0 : The installed externally signed SSL server certificate will expire on [arg1] and should be renewed or replaced immediately.**

  CMM security code has determined the externally signed SSL server certificate will expire in 10 days or less. The expiration date will be passed each time this event is logged. Failure to renew or replace this certificate will cause SSL clients to refuse connections to the CMM SSL servers.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0789

  User Response
  View the associated certificate at Mgt Module Management->Security->SSL Server Certificate->CMM SSL Server Certificate status: View Externally Signed Server Certificate. From same form use: "CMM Externally Signed SSL Server Certificate and Bundled Chain of Trust", to add renewed or new SSL server certificate immediately.

- **000160F1 : The installed externally signed SSL server certificate has expired as of [arg1]. Renew or replace this certificate immediately.**

  CMM security code has determined the externally signed SSL server certificate is expired. Clients connecting to the CMM will be forced to accept an untrusted connection which they may refuse to do based on policy.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0790

User Response
Use the following CMM form to renew the externally signed SSL server immediately and then import to restore client trust of CMM SSL servers. Mgt Module Management->Security->SSL Server Certificate-> "CMM Externally Signed SSL Server Certificate and Bundled Chain of Trust"

- **000160F2 : The installed externally signed LDAP client certificate will expire on [arg1] and should be renewed or replaced immediately.**

  CMM security code has determined the externally signed LDAP client certificate will expire in 10 days or less. The expiration date will be passed each time this event is logged. Failure to renew or replace this certificate will cause the LDAP server to refuse connections via the CMM LDAP client.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0791

  User Response
  You can view the associated certificate at Mgt Module Management->Security->LDAP Client Security->Signed LDAP Certificate status: View From same form use: "Generate and Import Externally Signed LDAP Client and Intermediate Certificate" button to add renewed or new LDP server certificate immediately.

- **000160F3 : The installed externally signed LDAP client certificate has expired as of [arg1]. Renew or replace this certificate immediately.**

  CMM security code has determined the externally signed LDAP client certificate is expired. LDAP servers requiring the CMM LDAP client to present a signed certificate will be forced to accept an untrusted connection which they may refuse to do based on policy.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0792

User Response
Use the following CMM form to renew the externally signed LDAP client certificate immediately and then import to restore LDAP server trust of the CMM LDAP client. Mgt Module Management->Security->LDAP Client Security-> "Generate and Import Externally Signed LDAP Client and Intermediate Certificate"

- **000160F4 : The SSL server certificate mode has been changed to [arg1] signed by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user changed the SSL server certificate mode to internally or externally.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0803

  User Response
  Information only; no action is required.

- **000160F5 : A new externally signed SSL [arg1] certificate with common name [arg2] has been installed by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user installed a new externally specified signed SSL certificate with the specified common name.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0804

  User Response
  Information only; no action is required.

- **000160F6 : External LDAP server CRL checking has been [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user changed the external LDAP Server CRL (Certificate Revocation List) checking to enabled or disabled.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0805

  User Response
  Information only; no action is required.
- **000160F7 : CRL [arg1] has been [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user imported or deleted the specified CRL (Certificate Revocation List).

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0806

  User Response
  Information only; no action is required.
- **000160F8 : The external LDAP server certificate with serial [arg1] was found on CRL [arg2], is no longer trusted and is revoked.**

  The external LDAP server certificate with the specified serial was found on the specified CRL (Certificate Revocation List) and is no longer trusted and is revoked.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support

No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0807

User Response
The LDAP server certificate must be updated to re-establish trust with CMM LDAP client.

- **000160F9 : Certificate using SHA1 hashing algorithm detected on Chassis Management Module.**

  Certificate using SHA1 hashing algorithm detected on Chassis Management Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0863

  User Response
  Browsers may not trust certificates using SHA1 hashing algorithm. It is reccomended that all certificates to use SHA256 hashing algorithm. Please regenerate all certificates using SHA256 hashing algorithm.

- **000160FA : Encapsulation mode was enabled on Chassis Management Module by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user changed encapsulation mode to enabled on Chassis Management Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0872

  User Response
  Information only; no action is required.

- **000160FB : Encapsulation mode was disabled on Chassis Management Module by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user changed encapsulation mode to disabled on Chassis Management Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0873

  User Response
  Information only; no action is required.
- **00016100 : Login failed because of expired password for user [arg1] from [arg2] at IP address [arg3].**

  The specified user cannot log in because the password has expired. Users (except SNMP and FTP users) will be prompted to change their passwords.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0628

  User Response
  Information only; no action is required.
- **00016101 : The SNMPv3 authentication protocol must be specified for SNMP users.**

  The security settings have been changed. Passwords are now required for all users. SNMPv3 users must specify authentication protocols.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support

No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0233

User Response
Each user must specify a password. Each SNMPv3 user must specify an authentication protocol (it cannot be set to None).

- **00016102 : Login failed because of a noncompliant password for user [arg1].**

  The password that is used to log in to the specified user account no longer meets the requirements for a password. Users (except SNMP and FTP users) will be prompted to change their passwords.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0153

  User Response
  Information only; no action is required.

- **00016106 : Remote login failed for user [arg1] from [arg2] at IP address [arg3] because all the external LDAP servers are unreachable.**

  The specified user cannot log in because all the external LDAP servers are unreachable.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0691

  User Response
  Information only; no action is required.

- **00016107 : Account has been locked for user [arg1] since [arg2].**

  The specified user account has been locked because of too many failed login attempts.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0700

  User Response
  Information only; no action is required.
- **00016109 : Account created for user [arg1] from USB Key.**

  The specified user account has been automatically created from USB Key attached to the Chassis Management Module (CMM). This occurs when there are zero accounts left on the CMM or all of the existing accounts are locked out. The account credentials are read from a pre-determined file on the USB key.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0687

  User Response
  Information only; no action is required.
- **00016110 : All local CMM user accounts have been disabled because the CMM was placed in central management mode by user ID [arg1] from [arg2] at IP address [arg3].**

  The CMM was placed into central management mode by the specified user. Consequently, all local user accounts that were previously defined on the CMM are now disabled and locked.

  Severity
  Informational

  Serviceable
  No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0433

User Response
Information only; no action is required.

- **00016111 : All local CMM user accounts have been enabled because the CMM was taken out of central management mode by user ID [arg1] from [arg2] at IP address [arg3].**

  The CMM was taken out of central management mode by the specified user. Consequently, all local user accounts that were previously defined on the CMM have been re-enabled and unlocked.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0434

  User Response
  Information only; no action is required.

- **00016112 : Node Account created for user [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has created the specified centrally managed node account.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0843

  User Response
  Information only; no action is required.

- **00016113 : Node Account deleted for user [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has deleted the specified centrally managed node account.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0844

  User Response
  Information only; no action is required.
- **00016114 : All Node Accounts deleted by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has deleted all centrally managed node accounts.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0845

  User Response
  Information only; no action is required.
- **00016120 : Node bay [arg1] node name was changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the vital product data in the node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0059

User Response
Information only; no action is required.

- **00016124 : Default account password must be changed on next login setting was disabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has disabled the "Factory default 'USERID' account password must be changed on next login" setting. This setting determines that the USERID account must not change the password the next time the password is used to log in to the Chassis Management Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0981

  User Response
  Information only; no action is required.

- **00016126 : Complex password rules setting was disabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has disabled the "Complex password rules" setting. This setting determines the type of password that is acceptable.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0983

  User Response
  Information only; no action is required.

- **00016128 : Force user to change password on first login setting was disabled by user ID [arg1] from [arg2] at IP address [arg3].**

The specified user has disabled the "Force user to change password on first access" setting. The user must not change the password the next time the user logs in to the Chassis Management Module.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0985

User Response
Information only; no action is required.

- **00016201 : Node bay data for node bay [arg1] uploaded to Chassis Management Module.**

Bay data for the specified node bay has been uploaded to the Chassis Management Module (CMM). This data is stored in the CMM nonvolatile RAM (NVRAM) and is associated with the node bay.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0564

User Response
Information only; no action is required.

- **00016202 : Node bay data for node bay [arg1] uploaded to Chassis Management Module.**

Bay data for the specified node bay has been uploaded to the Chassis Management Module (CMM). This data is stored in the CMM nonvolatile RAM (NVRAM) and is associated with the node bay.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category

Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0564

User Response
Information only; no action is required.

- **00016203 : Node bay data for node bay [arg1] uploaded to Chassis Management Module.**

  Bay data for the specified node bay has been uploaded to the Chassis Management Module (CMM). This data is stored in the CMM nonvolatile RAM (NVRAM) and is associated with the node bay.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0564

  User Response
  Information only; no action is required.

- **00016204 : Node bay data for node bay [arg1] uploaded to Chassis Management Module.**

  Bay data for the specified node bay has been uploaded to the Chassis Management Module (CMM). This data is stored in the CMM nonvolatile RAM (NVRAM) and is associated with the node bay.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0564

  User Response
  Information only; no action is required.

- **00016205 : Node bay data for node bay [arg1] uploaded to Chassis Management Module.**

  Bay data for the specified node bay has been uploaded to the Chassis Management Module (CMM). This data is stored in the CMM nonvolatile RAM (NVRAM) and is associated with the node bay.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0564

User Response
Information only; no action is required.

- **00016206 : Node bay data for node bay [arg1] uploaded to Chassis Management Module.**

  Bay data for the specified node bay has been uploaded to the Chassis Management Module (CMM). This data is stored in the CMM nonvolatile RAM (NVRAM) and is associated with the node bay.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0564

  User Response
  Information only; no action is required.

- **00016207 : Node bay data for node bay [arg1] uploaded to Chassis Management Module.**

  Bay data for the specified node bay has been uploaded to the Chassis Management Module (CMM). This data is stored in the CMM nonvolatile RAM (NVRAM) and is associated with the node bay.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0564

User Response
Information only; no action is required.

- **00016208 : Node bay data for node bay [arg1] uploaded to Chassis Management Module.**

  Bay data for the specified node bay has been uploaded to the Chassis Management Module (CMM). This data is stored in the CMM nonvolatile RAM (NVRAM) and is associated with the node bay.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0564

  User Response
  Information only; no action is required.

- **00016209 : Node bay data for node bay [arg1] uploaded to Chassis Management Module.**

  Bay data for the specified node bay has been uploaded to the Chassis Management Module (CMM). This data is stored in the CMM nonvolatile RAM (NVRAM) and is associated with the node bay.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0564

  User Response
  Information only; no action is required.

- **0001620A : Node bay data for node bay [arg1] uploaded to Chassis Management Module.**

  Bay data for the specified node bay has been uploaded to the Chassis Management Module (CMM). This data is stored in the CMM nonvolatile RAM (NVRAM) and is associated with the node bay.

  Severity
  Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0564

User Response
Information only; no action is required.

- **0001620B : Node bay data for node bay [arg1] uploaded to Chassis Management Module.**

  Bay data for the specified node bay has been uploaded to the Chassis Management Module (CMM). This data is stored in the CMM nonvolatile RAM (NVRAM) and is associated with the node bay.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0564

  User Response
  Information only; no action is required.

- **0001620C : Node bay data for node bay [arg1] uploaded to Chassis Management Module.**

  Bay data for the specified node bay has been uploaded to the Chassis Management Module (CMM). This data is stored in the CMM nonvolatile RAM (NVRAM) and is associated with the node bay.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0564

User Response
Information only; no action is required.

- **0001620D : Node bay data for node bay [arg1] uploaded to Chassis Management Module.**

  Bay data for the specified node bay has been uploaded to the Chassis Management Module (CMM). This data is stored in the CMM nonvolatile RAM (NVRAM) and is associated with the node bay.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0564

  User Response
  Information only; no action is required.

- **0001620E : Node bay data for node bay [arg1] uploaded to Chassis Management Module.**

  Bay data for the specified node bay has been uploaded to the Chassis Management Module (CMM). This data is stored in the CMM nonvolatile RAM (NVRAM) and is associated with the node bay.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0564

  User Response
  Information only; no action is required.

- **00016301 : Node bay data for node bay [arg1] changed by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the node bay data for the specified node.

  Severity
  Informational

  Serviceable
  No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0565

User Response
Information only; no action is required.

- **00016302 : Node bay data for node bay [arg1] changed by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the node bay data for the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0565

  User Response
  Information only; no action is required.

- **00016303 : Node bay data for node bay [arg1] changed by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the node bay data for the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0565

  User Response
  Information only; no action is required.

- **00016304 : Node bay data for node bay [arg1] changed by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the node bay data for the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0565

  User Response
  Information only; no action is required.
- **00016305 : Node bay data for node bay [arg1] changed by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the node bay data for the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0565

  User Response
  Information only; no action is required.
- **00016306 : Node bay data for node bay [arg1] changed by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the node bay data for the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0565

User Response
Information only; no action is required.

- **00016307 : Node bay data for node bay [arg1] changed by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the node bay data for the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0565

  User Response
  Information only; no action is required.

- **00016308 : Node bay data for node bay [arg1] changed by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the node bay data for the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0565

  User Response
  Information only; no action is required.

- **00016309 : Node bay data for node bay [arg1] changed by user ID [arg2] from [arg3] at IP address [arg4].**

The specified user has changed the node bay data for the specified node.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0565

User Response
Information only; no action is required.

- **0001630A : Node bay data for node bay [arg1] changed by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the node bay data for the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0565

  User Response
  Information only; no action is required.

- **0001630B : Node bay data for node bay [arg1] changed by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the node bay data for the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0565

User Response
Information only; no action is required.

- **0001630C : Node bay data for node bay [arg1] changed by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the node bay data for the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0565

  User Response
  Information only; no action is required.

- **0001630D : Node bay data for node bay [arg1] changed by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the node bay data for the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0565

  User Response
  Information only; no action is required.

- **0001630E : Node bay data for node bay [arg1] changed by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the node bay data for the specified node.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0565

User Response
Information only; no action is required.

- **00016310 : SLP mode successfully changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the address type of the Service Location Protocol (SLP) server.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0380

  User Response
  Information only; no action is required.

- **00016311 : SLP address successfully changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the IP address of the Service Location Protocol (SLP) server.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0381

User Response
Information only; no action is required.

- **00016400 : Invalid encryption keys detected. Regenerating encryption keys. Verify local login profile configurations.**

  The Chassis Management Module has detected that encryption keys are not valid. It will regenerate encryption keys.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0459

  User Response
  Information only; no action is required.

- **00016410 : SNMP system contact name changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the SNMP system contact name.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0290

  User Response
  Information only; no action is required.

- **00016411 : SNMP system location changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the SNMP system location.

  Severity
  Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0291

User Response
Information only; no action is required.

- **00016412 : SNMPv1 community [arg1] IP address or host name [arg2] changed to [arg3] by user ID [arg4] from [arg5] at IP address [arg6].**

  The specified user has changed the host name or IP address that is associated with an SNMP version 1 community.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0292

  User Response
  Information only; no action is required.

- **00016413 : Domain name service (DNS) enabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has activated the DNS service.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0293

User Response
Information only; no action is required.

- **00016414 : Domain name service (DNS) disabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has deactivated the DNS service.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0294

  User Response
  Information only; no action is required.

- **00016415 : Domain name service (DNS) IP address [arg1] changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed a DNS host name value.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0295

  User Response
  Information only; no action is required.

- **00016416 : TCP/IP host table entry [arg1] host name value changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the Chassis Management Module host name of an entry in the TCP/IP host table.

  Severity
  Informational

  Serviceable
  No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0296

User Response
Information only; no action is required.

- **00016418 : SMTP server name or IP address changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the SMTP server host name or IP address.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0298

  User Response
  Information only; no action is required.

- **00016419 : SMTP customer selectable email content value changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the SMTP client selectable email content value.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0299

  User Response
  Information only; no action is required.

- **0001641A : Ping IP address changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the ping host IP address.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0300

  User Response
  Information only; no action is required.
- **0001641B : Ping timeout value changed to [arg1] seconds by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the ping timeout value.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0301

  User Response
  Information only; no action is required.
- **0001641C : LDAP server [arg1] host name or IP address changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the host name or IP address of an LDAP server.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category

User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0302

User Response
Information only; no action is required.

- **0001641D : LDAP server [arg1] port number changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the port number of the LDAP client to connect to an LDAP server.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0303

  User Response
  Information only; no action is required.

- **0001641E : LDAP root directory entry distinguished name (DN) changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the root distinguished name that is used by the LDAP client.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0304

  User Response
  Information only; no action is required.

- **0001641F : LDAP user directory search base distinguished name (DN) changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

The specified user has changed the base distinguished name that is used by the LDAP client for user searches.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0305

User Response
Information only; no action is required.

- **00016420 : LDAP group search base distinguished name (DN) changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the base distinguished name that is used by the LDAP client for group searches.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0306

  User Response
  Information only; no action is required.

- **00016421 : LDAP SSL use set to [arg1] (enabled) by user ID [arg2] from [arg3] at IP address [arg4].**

  The LDAP client is configured to use Secure Sockets Layer (SSL) as the connection method to LDAP servers.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0307

User Response
Information only; no action is required.

- **00016422 : LDAP SSL use set to [arg1] (disabled) by user ID [arg2] from [arg3] at IP address [arg4].**

  The LDAP client is not configured to use Secure Sockets Layer (SSL) as the connection method to LDAP servers.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0308

  User Response
  Information only; no action is required.

- **00016423 : LDAP client binding method changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the binding method that is used by the LDAP client.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0309

  User Response
  Information only; no action is required.

- **00016424 : LDAP client distinguished name (DN) changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

The specified user has changed the distinguished name that is used by the LDAP client to bind to the LDAP server.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0310

User Response
Information only; no action is required.

- **00016425 : LDAP client password changed by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has changed the password that is used by the LDAP client to authenticate to the LDAP server.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0311

  User Response
  Information only; no action is required.

- **00016426 : LDAP group filter value was changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the LDAP client group filter value.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category

User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0677

User Response
Information only; no action is required.

- **00016427 : LDAP user ID search attribute value changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the LDAP client user ID search attribute value.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0313

  User Response
  Information only; no action is required.

- **00016428 : LDAP server address detection method set to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the method that is used by the LDAP client to select an LDAP service host.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0314

  User Response
  Information only; no action is required.

- **00016429 : LDAP login permissions attribute changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

The specified user has changed the login permission attribute value that is used by the LDAP client.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0315

User Response
Information only; no action is required.

- **0001642A : LDAP authentication domain value changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the authentication domain value that is used by the LDAP client.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0316

  User Response
  Information only; no action is required.

- **0001642B : LDAP role based security model set to [arg1] (enabled) by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has enabled the use of role-based security by the LDAP client.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0317

User Response
Information only; no action is required.

- **0001642C : LDAP role based security model set to [arg1] (disabled) by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has disabled the use of role-based security by the LDAP client.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0318

  User Response
  Information only; no action is required.

- **0001642D : LDAP server role based security target name value changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the role-based security target name that is used for the LDAP server by the LDAP client.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0319

  User Response
  Information only; no action is required.

- **0001642E : Advanced failover IP mode disabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has disabled advanced failover IP mode.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0320

User Response
Information only; no action is required.

- **0001642F : Advanced failover IP mode set to not swap IP addresses between the standby and primary Chassis Management Modules by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has set advanced failover IP mode. If the primary Chassis Management Module (CMM) fails, the primary CMM and the standby CMM will retain their IP addresses. IP addresses will not be swapped during failover.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0322

  User Response
  Information only; no action is required.

- **00016430 : Advanced failover IP mode set to swap IP addresses between the standby and primary Chassis Management Modules by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has set advanced failover IP mode. If the primary Chassis Management Module (CMM) fails, IP addresses will be swapped between the primary CMM and the standby CMM.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category

User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0321

User Response
Information only; no action is required.

- **00016500 : File transfer failed for user [arg1] from [arg2]. [arg3].**

The file cannot be transferred to the Chassis Management Module. This local file is typically used to store switch firmware for later distribution or service data information.

Severity
Informational

Serviceable
Yes

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0462

User Response
Complete the following steps until the problem is solved:

1. Make sure that you have entered the file name correctly and that permissions have been set correctly.
2. Make sure that the file is visible on the network.
3. Make sure that the Chassis Management Module (CMM) has sufficient space to store the file. In the CMM user interface, click "Mgt Module Management" and "File Management" to display information about how much space is available. A list of files that can be deleted to make more space is also displayed.
4. Try to transfer the data again.

- **00016601 : VLAN Global enabled by user ID [arg1] from [arg2] at IP address [arg3].**

The specified user has enabled Global VLAN. VLAN support can be enabled or disabled globally.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0720

User Response
Information only; no action is required.

- **00016602 : VLAN Global disabled by user ID [arg1] from [arg2] at IP address [arg3].**

The specified user has disabled Global VLAN. VLAN support can be enabled or disabled globally.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0721

User Response
Information only; no action is required.

- **00016603 : VLAN configuration committed by user ID [arg1] from [arg2] at IP address [arg3].**

The specified user has committed the temporary VLAN configuration.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0722

User Response
Information only; no action is required.

- **00016604 : VLAN temporary commit timeout changed [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

The specified user has changed the VLAN configuration timeout after which the temporary configuration expires.

Severity
Informational

Serviceable

No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0723

User Response
Information only; no action is required.

- **00016605 : VLAN temporary commit timeout has expired. Reverted to the last commited VLAN configuration.**

  The VLAN temporary commit timeout has expired. Reverted to the last commited VLAN configuration.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0724

  User Response
  Information only; no action is required.

- **0001660A : VLAN [arg1] SOL feature was enabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has enabled the SOL feature on the specified VLAN entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0934

  User Response

Information only; no action is required.

- **0001660B : VLAN [arg1] SOL feature was disabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has disabled the SOL feature on the specified VLAN entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0935

  User Response
  Information only; no action is required.

- **0001660C : VLAN [arg1] Tagging feature was enabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has enabled the Tagging feature on the specified VLAN entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0936

  User Response
  Information only; no action is required.

- **0001660D : VLAN [arg1] Tagging feature was disabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has disabled the Tagging feature on the specified VLAN entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0937

User Response
Information only; no action is required.

- **0001660E : VLAN [arg1] has IPv4 address changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IPv4 address of the CMM VLAN entry configuration.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0729

  User Response
  Information only; no action is required.

- **0001660F : VLAN [arg1] has IPv4 mask changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IPv4 mask of the CMM VLAN entry configuration.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0730

  User Response
  Information only; no action is required.

- **00016610 : VLAN [arg1] has IPv4 gateway changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

The specified user has changed the IPv4 gateway address of the CMM VLAN entry configuration.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0731

User Response
Information only; no action is required.

- **00016611 : VLAN [arg1] has vlan ID changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the VLAN ID of the CMM VLAN entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0732

  User Response
  Information only; no action is required.

- **00016612 : VLAN [arg1] has name changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the name of the CMM VLAN entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0733

User Response
Information only; no action is required.

- **00016613 : VLAN [arg1] has Tagging changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the tagging configuration of the CMM VLAN entry to tagged/untagged.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0735

  User Response
  Information only; no action is required.

- **00016614 : VLAN [arg1] state was restarted by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has restarted the state of the specified CMM VLAN entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0958

  User Response
  Information only; no action is required.

- **00016615 : VLAN [arg1] has subnet route 1 changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IPv4 subnet route 1 address of the CMM VLAN entry configuration.

  Severity

Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0736

User Response
Information only; no action is required.

- **00016616 : VLAN [arg1] has subnet route 2 changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IPv4 subnet route 2 address of the CMM VLAN entry configuration.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0737

  User Response
  Information only; no action is required.

- **00016617 : VLAN [arg1] has subnet route 3 changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IPv4 subnet route 3 address of the CMM VLAN entry configuration.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0738

User Response
Information only; no action is required.

- **00016618 : VLAN [arg1] has subnet route mask 1 changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IPv4 subnet route mask 1 address of the CMM VLAN entry configuration.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0739

  User Response
  Information only; no action is required.

- **00016619 : VLAN [arg1] has subnet route mask 2 changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IPv4 subnet route mask 2 address of the CMM VLAN entry configuration.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0740

  User Response
  Information only; no action is required.

- **0001661A : VLAN [arg1] has subnet route mask 3 changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IPv4 subnet route mask 3 address of the CMM VLAN entry configuration.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0741

User Response
Information only; no action is required.

- **0001661B : VLAN [arg1] has IPv6 subnet route 1 changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IPv6 subnet route 1 address of the CMM VLAN entry configuration.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0762

  User Response
  Information only; no action is required.

- **0001661C : VLAN [arg1] has IPv6 subnet route 2 changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IPv6 subnet route 2 address of the CMM VLAN entry configuration.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0763

User Response
Information only; no action is required.

- **0001661D : VLAN [arg1] has IPv6 subnet route 3 changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IPv6 subnet route 3 address of the CMM VLAN entry configuration.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0764

  User Response
  Information only; no action is required.

- **0001661E : VLAN [arg1] has IPv6 subnet route prefix length 1 changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IPv6 subnet route prefix length 1 of the CMM VLAN entry configuration.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0765

  User Response
  Information only; no action is required.

- **0001661F : VLAN [arg1] has IPv6 subnet route prefix length 2 changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IPv6 subnet route prefix length 2 of the CMM VLAN entry configuration.

  Severity

Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0766

User Response
Information only; no action is required.

- **00016620 : VLAN [arg1] has IPv6 subnet route prefix length 3 changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IPv6 subnet route prefix length 2 of the CMM VLAN entry configuration.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0767

  User Response
  Information only; no action is required.

- **00016621 : VLAN [arg1] has IPv6 address changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IPv6 address of the CMM VLAN entry configuration.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0772

User Response
Information only; no action is required.

- **00016622 : VLAN [arg1] has IPv6 prefix length changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IPv6 prefix length of the CMM VLAN entry configuration.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0773

  User Response
  Information only; no action is required.

- **00016623 : VLAN [arg1] has IPv6 gateway changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IPv6 gateway address of the CMM VLAN entry configuration.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0774

  User Response
  Information only; no action is required.

- **00016624 : VLAN [arg1] state was enabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has enabled the state of the specified CMM VLAN entry.

  Severity
  Informational

  Serviceable

No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0959

User Response
Information only; no action is required.

- **00016625 : VLAN [arg1] state was disabled by user ID [arg2] from [arg3] at IP address [arg4].**

The specified user has disabled the state of the specified CMM VLAN entry.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0960

User Response
Information only; no action is required.

- **00016626 : VLAN [arg1] state was added by user ID [arg2] from [arg3] at IP address [arg4].**

The specified user has added the state of the specified CMM VLAN entry.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0961

User Response
Information only; no action is required.

- **00016627 : VLAN [arg1] state was deleted by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has deleted the state of the specified CMM VLAN entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0962

  User Response
  Information only; no action is required.
- **00016651 : VLAN [arg1] has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has enabled/disabled the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0726

  User Response
  Information only; no action is required.
- **00016652 : VLAN [arg1] has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has enabled/disabled the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0726

User Response
Information only; no action is required.

- **00016653 : VLAN [arg1] has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has enabled/disabled the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0726

  User Response
  Information only; no action is required.

- **00016654 : VLAN [arg1] has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has enabled/disabled the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0726

  User Response
  Information only; no action is required.

- **00016655 : VLAN [arg1] has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has enabled/disabled the specified VLAN node entry.

  Severity
  Informational

  Serviceable

No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0726

User Response
Information only; no action is required.

- **00016656 : VLAN [arg1] has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has enabled/disabled the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0726

  User Response
  Information only; no action is required.

- **00016657 : VLAN [arg1] has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has enabled/disabled the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0726

  User Response
  Information only; no action is required.

- **00016658 : VLAN [arg1] has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has enabled/disabled the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0726

  User Response
  Information only; no action is required.
- **00016659 : VLAN [arg1] has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has enabled/disabled the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0726

  User Response
  Information only; no action is required.
- **0001665A : VLAN [arg1] has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has enabled/disabled the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0726

User Response
Information only; no action is required.

- **0001665B : VLAN [arg1] has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has enabled/disabled the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0726

  User Response
  Information only; no action is required.

- **0001665C : VLAN [arg1] has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has enabled/disabled the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0726

  User Response
  Information only; no action is required.

- **0001665D : VLAN [arg1] has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has enabled/disabled the specified VLAN node entry.

  Severity
  Informational

  Serviceable

No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0726

User Response
Information only; no action is required.

- **0001665E : VLAN [arg1] has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has enabled/disabled the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0726

  User Response
  Information only; no action is required.

- **00016661 : VLAN [arg1] has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has enabled/disabled the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0726

  User Response
  Information only; no action is required.

- **00016662 : VLAN [arg1] has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has enabled/disabled the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0726

  User Response
  Information only; no action is required.
- **00016663 : VLAN [arg1] has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has enabled/disabled the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0726

  User Response
  Information only; no action is required.
- **00016664 : VLAN [arg1] has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has enabled/disabled the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0726

User Response
Information only; no action is required.

- **00016665 : VLAN [arg1] has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has enabled/disabled the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0726

  User Response
  Information only; no action is required.

- **00016666 : VLAN [arg1] has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has enabled/disabled the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0726

  User Response
  Information only; no action is required.

- **00016667 : VLAN [arg1] has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has enabled/disabled the specified VLAN node entry.

  Severity
  Informational

  Serviceable

No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0726

User Response
Information only; no action is required.

- **00016668 : VLAN [arg1] has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has enabled/disabled the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0726

  User Response
  Information only; no action is required.

- **00016669 : VLAN [arg1] has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has enabled/disabled the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0726

  User Response
  Information only; no action is required.

- **0001666A : VLAN [arg1] has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has enabled/disabled the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0726

  User Response
  Information only; no action is required.
- **0001666B : VLAN [arg1] has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has enabled/disabled the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0726

  User Response
  Information only; no action is required.
- **0001666C : VLAN [arg1] has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has enabled/disabled the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0726

User Response
Information only; no action is required.

- **0001666D : VLAN [arg1] has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has enabled/disabled the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0726

  User Response
  Information only; no action is required.

- **0001666E : VLAN [arg1] has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has enabled/disabled the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0726

  User Response
  Information only; no action is required.

- **00016671 : VLAN [arg1] VID has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the VLAN ID to the specified value for the specified VLAN node entry.

  Severity
  Informational

  Serviceable

No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0727

User Response
Information only; no action is required.

- **00016672 : VLAN [arg1] VID has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the VLAN ID to the specified value for the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0727

  User Response
  Information only; no action is required.

- **00016673 : VLAN [arg1] VID has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the VLAN ID to the specified value for the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0727

  User Response
  Information only; no action is required.

- **00016674 : VLAN [arg1] VID has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the VLAN ID to the specified value for the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0727

  User Response
  Information only; no action is required.
- **00016675 : VLAN [arg1] VID has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the VLAN ID to the specified value for the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0727

  User Response
  Information only; no action is required.
- **00016676 : VLAN [arg1] VID has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the VLAN ID to the specified value for the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0727

User Response
Information only; no action is required.

- **00016677 : VLAN [arg1] VID has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

The specified user has changed the VLAN ID to the specified value for the specified VLAN node entry.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0727

User Response
Information only; no action is required.

- **00016678 : VLAN [arg1] VID has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

The specified user has changed the VLAN ID to the specified value for the specified VLAN node entry.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0727

User Response
Information only; no action is required.

- **00016679 : VLAN [arg1] VID has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

The specified user has changed the VLAN ID to the specified value for the specified VLAN node entry.

Severity
Informational

Serviceable

No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0727

User Response
Information only; no action is required.

- **0001667A : VLAN [arg1] VID has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the VLAN ID to the specified value for the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0727

  User Response
  Information only; no action is required.

- **0001667B : VLAN [arg1] VID has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the VLAN ID to the specified value for the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0727

User Response
Information only; no action is required.

- **0001667C : VLAN [arg1] VID has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the VLAN ID to the specified value for the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0727

  User Response
  Information only; no action is required.

- **0001667D : VLAN [arg1] VID has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the VLAN ID to the specified value for the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0727

  User Response
  Information only; no action is required.

- **0001667E : VLAN [arg1] VID has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the VLAN ID to the specified value for the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0727

User Response
Information only; no action is required.

- **00016681 : VLAN [arg1] Name has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the name to the specified value for the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0728

  User Response
  Information only; no action is required.

- **00016682 : VLAN [arg1] Name has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the name to the specified value for the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0728

  User Response
  Information only; no action is required.

- **00016683 : VLAN [arg1] Name has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the name to the specified value for the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0728

  User Response
  Information only; no action is required.
- **00016684 : VLAN [arg1] Name has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the name to the specified value for the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0728

  User Response
  Information only; no action is required.
- **00016685 : VLAN [arg1] Name has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the name to the specified value for the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0728

User Response
Information only; no action is required.

- **00016686 : VLAN [arg1] Name has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the name to the specified value for the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0728

  User Response
  Information only; no action is required.

- **00016687 : VLAN [arg1] Name has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the name to the specified value for the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0728

  User Response
  Information only; no action is required.

- **00016688 : VLAN [arg1] Name has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

The specified user has changed the name to the specified value for the specified VLAN node entry.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0728

User Response
Information only; no action is required.

- **00016689 : VLAN [arg1] Name has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the name to the specified value for the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0728

  User Response
  Information only; no action is required.

- **0001668A : VLAN [arg1] Name has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the name to the specified value for the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0728

User Response
Information only; no action is required.

- **0001668B : VLAN [arg1] Name has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the name to the specified value for the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0728

  User Response
  Information only; no action is required.

- **0001668C : VLAN [arg1] Name has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the name to the specified value for the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0728

  User Response
  Information only; no action is required.

- **0001668D : VLAN [arg1] Name has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the name to the specified value for the specified VLAN node entry.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0728

User Response
Information only; no action is required.

- **0001668E : VLAN [arg1] Name has changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the name to the specified value for the specified VLAN node entry.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0728

  User Response
  Information only; no action is required.

- **00016699 : Call Home disabled by user ID [arg1] from [arg2] at IP address [arg3].**

  Automatic support notifications functionality has been disabled.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0828

User Response
Information only; no action is required.

- **00016700 : Call Home enabled by user ID [arg1] from [arg2] at IP address [arg3].**

  Automatic support notifications functionality has been enabled. If automatic support notifications are enabled, a test notification will be generated automatically.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0836

  User Response
  Information only; no action is required.

- **00016702 : An HTTP proxy setting for call home was changed by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has changed the HTTP proxy that is used for automatic support notification.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0340

  User Response
  Information only; no action is required.

- **00016704 : Terms and conditions of call home have been accepted by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has accepted the terms and conditions agreement for automatic support notifications.

  Severity
  Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0359

User Response
Information only; no action is required.

- **00016705 : Call home parameter [arg1] was changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the automatic support notification configuration.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0365

  User Response
  Information only; no action is required.

- **00016706 : Call home configuration for [arg1] is invalid and not saved.**

  A user has tried to save incorrect configuration data that is required for automatic support notifications. Invalid data will not be saved.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0360

User Response
Information only; no action is required.

- **00016800 : Service request number [arg1] was created for event [arg2].**

  An automatic support notification of the specified event was successful, and the specified service request has been generated.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0361

  User Response
  Information only; no action is required.

- **00016801 : Event [arg1] call home failed. Reason: [arg2].**

  A confirmation has not been received from the destination of the automatic support notification.

  Severity
  Informational

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0855

  User Response
  Complete the following steps until the problem is solved:

  1. Check the network connectivity between the Chassis Management Module and the external network.
  2. Submit a test service request to validate connectivity.
  3. Save the service data locally.

- **00016802 : Test call home by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has generated a test service request.

  Severity
  Informational

Serviceable
No

Automatically notify support
Yes

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0363

User Response
Information only; no action is required.

- **00016803 : Manual call home generated by user ID [arg1] from [arg2] at IP address [arg3]. Message: [arg4].**

  The specified user has submitted a service request. A service data log is being submitted to Support for review with an open service request number.

  Severity
  Informational

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0364

  User Response
  Support will address the problem.

- **00016804 : Service data collection initiated on CMM [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  Service data collection initiated on specified CMM by the specified user account.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information

Prefix: CMM **ID:** 0271

User Response
Information only; no action is required.

- **00016805 : Service data collection initiated on CMM [arg1] by user ID [arg2] from [arg3] at IP address [arg4] is done.**

  Service data collection initiated on specified CMM by the specified user account is done.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0856

  User Response
  Information only; no action is required.

- **00016806 : Service data collection failed on CMM [arg1] with error code [arg2].**

  Service data collection failed on specified CMM with the specified error code.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0273

  User Response
  Information only; no action is required.

- **00016807 : Service data collection completed on CMM [arg1].**

  Service data collection completed on specified CMM.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support

No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0858

User Response
Information only; no action is required.

- **00017002 : Chassis Management Module reset: [arg1].**

The Chassis Management Module has been reset. The logs provide additional details.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0463

User Response
Information only; no action is required.

- **00017003 : There are no valid login profiles. Resetting login profile 1 to factory defaults.**

The Chassis Management Module (CMM) requires at least one valid login profile (user account). If none are found, the first user profile will be enabled with the default user name and password.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0464

User Response
Information only; no action is required.

- **00017004 : There are no login profiles with Supervisor or User Account Management roles.**

The Chassis Management Module (CMM) requires that at least one login profile (user account) have the authority to manage user accounts. Therefore, the CMM has given that authority to the specified user account.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0465

User Response
Information only; no action is required.

- **00017100 : Node in bay [arg1] was requested to shut down the operating system and power off by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has requested that the operating system for the specified node be shut down and the specified node be powered off.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0946

  User Response
  Information only; no action is required.

- **00017101 : Node in bay [arg1] was requested to reset to diagnostics (NMI) by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has requested a nonmaskable interrupt (NMI) reset for a specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0947

User Response
Information only; no action is required.

- **00017103 : Both Chassis Management Modules are active. Resetting Chassis Management Modules.**

  Both Chassis Management Modules (CMMs) are identified as primary, so both CMMs will be reset.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0513

  User Response
  Information only; no action is required.

- **00017104 : CMM bay location cannot be determined, defaulting to CMM bay 2.**

  The Chassis Management Module (CMM) is unable to determine the CMM bay in which it is installed. It will default to assume that it is in CMM bay 2.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0012

  User Response
  Do not move the CMM to another bay. Inspect the CMM connector. If there is no damage, replace the CMM. If there is damage, replace the affected parts.

- **00017105 : Chassis Management Module switch over from bay 1 to bay 2.**

The Chassis Management Module (CMM) in CMM bay 1 has failed over to the CMM in CMM bay 2. The CMM in CMM bay 2 is now the primary CMM.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0510

User Response
Check the CMM event log for other events that are related to the CMM in CMM bay 1, and solve those events.

- **00017106 : Chassis Management Module switch over from bay 2 to bay 1.**

The Chassis Management Module (CMM) in CMM bay 2 has failed over to the CMM in CMM bay 1. The CMM in CMM bay 1 is now the primary CMM.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0511

User Response
Check the CMM event log for other events that are related to the CMM in CMM bay 2, and solve those events.

- **00017107 : Node [arg1] power state restored after an unexpected power loss.**

The power state of the specified node has been restored after an unexpected power loss.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0176

User Response
Check the Chassis Management Module event log for other events that might be related to the node or to power supplies.

- **00017108 : Ethernet [[arg1]] interface is up for the primary Chassis Management Module.**

The Chassis Management Module external Ethernet interface is up.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0071

User Response
Information only; no action is required.

- **00017109 : Ethernet [[arg1]] interface is down for the primary Chassis Management Module.**

The Chassis Management Module external Ethernet interface is down. Devices internal to the chassis on the management network, such as system-management processors and the Flex System Manager management module, will also lose network connectivity.

Severity
Informational

Serviceable
Yes

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0072

User Response
Complete the following steps until the problem is solved:

1. Make sure that the external Ethernet cable is connected at both ends.

2. Make sure that the cable is working:
   a. Swap both ends of the cable.
   b. Make sure that the link LED on the RJ-45 connector is lit on the Chassis Management Module (CMM) and on the network device to which the CMM is attached.
3. Make sure that the network switch has power.
4. Make sure that the network infrastructure is operational.

- **0001710D : I/O module [arg1] Protected mode configured by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the Protected mode setting in the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0189

  User Response
  Information only; no action is required.

- **0001710E : Firmware update detected for the system-management processor on [arg1].**

  The system-management processor firmware in the specified node is being updated.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0177

  User Response
  Do not reset the system-management processor, remove the node, or perform a service-level reset of the node when the node is in update mode.

- **0001710F : I/O module [arg1] has restarted.**

  The I/O module has been restarted.

  Severity

Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0190

User Response
Information only; no action is required.

- **00017111 : File [arg1] uploaded from [arg2] client by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has uploaded a file to the Chassis Management Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0384

  User Response
  Information only; no action is required.

- **00017112 : Configuration restored from a configuration file by user [arg1] from [arg2] at IP address [arg3].**

  The specified user has restored the Chassis Management Module (CMM) configuration from a previously saved configuration file. Some configuration settings might require that the CMM be restarted before they take effect.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0512

User Response
Information only; no action is required.

- **00017113 : Ethernet DHCP host name=[arg1], DN=[arg2], IP=[arg3], GW=[arg4], SN=[arg5], DNS1=[arg6].**

  The external Ethernet port on the Chassis Management Module is using a DHCP IP address for the specified host name. The host name, IP address, gateway address, and network mask are provided.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0073

  User Response
  Information only; no action is required.

- **00017114 : Ethernet host name=[arg1], IP=[arg2], GW=[arg3], Mask=[arg4].**

  The external Ethernet port on the Chassis Management Module is using a static IP address for the specified host name. The host name, IP address, gateway address, and network mask are provided.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0074

  User Response
  Information only; no action is required.

- **00017115 : DHCP setting of the primary CMM network interface has been changed from [arg1] to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the DHCP setting of the Chassis Management Module external network interface.

  Severity

Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0516

User Response
Information only; no action is required.

- **00017116 : Host name on [arg1] CMM has been changed from [arg2] to [arg3] by user ID [arg4] from [arg5] at IP address [arg6].**

  The specified user has changed the host name of the Chassis Management Module to the specified value.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0518

  User Response
  Information only; no action is required.

- **00017117 : IP address of the [arg1] CMM network interface has been changed from [arg2] to [arg3] by user ID [arg4] from [arg5] at IP address [arg6].**

  The specified user has changed the IP address of the Chassis Management Module external network interface to the specified value.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Network change (Informational)

  SNMP Trap ID
  mmTrapNwChangeS

CIM Information
Prefix: CMM **ID:** 0662

User Response
Information only; no action is required.

- **00017118 : Ethernet data rate of the primary CMM network interface has been changed from [arg1] to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the Ethernet data rate of the primary Chassis Management Module external network interface to the specified value.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0519

  User Response
  Information only; no action is required.

- **00017119 : Ethernet duplex setting of the primary CMM network interface has been changed from [arg1] to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the Ethernet duplex setting of the primary Chassis Management Module external network interface to the specified value.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0520

  User Response
  Information only; no action is required.

- **0001711A : Ethernet locally administered MAC address of the primary CMM network interface has been changed from [arg1] to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the Ethernet locally administered MAC address of the primary Chassis Management Module external network interface to the specified value.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0521

User Response
Information only; no action is required.

- **0001711B : Gateway address of the primary CMM network interface has been changed from [arg1] to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the gateway address of the primary Chassis Management Module external network interface to the specified value.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Network change (Informational)

  SNMP Trap ID
  mmTrapNwChangeS

  CIM Information
  Prefix: CMM **ID:** 0522

  User Response
  Information only; no action is required.

- **0001711C : Ethernet MTU setting of the primary CMM network interface has been changed from [arg1] to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the Ethernet maximum transmission unit (MTU) setting of the primary Chassis Management Module external network interface to the specified value.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0523

User Response
Information only; no action is required.

- **0001711D : Subnet mask of the primary CMM network interface has been changed from [arg1] to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the subnet mask of the primary Chassis Management Module external network interface to the specified value.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Network change (Informational)

  SNMP Trap ID
  mmTrapNwChangeS

  CIM Information
  Prefix: CMM **ID:** 0524

  User Response
  Information only; no action is required.

- **00017127 : Ethernet host name=[arg1], floating IP=[arg2], GW=[arg3], Mask=[arg4].**

  The external Ethernet port on the Chassis Management Module is using a floating IP address for the specified host name. The host name, floating IP address, gateway address, and network mask are provided.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0641

  User Response
  Information only; no action is required.

- **00017128 : Floating IP address of the primary CMM network interface has been changed from [arg1] to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

The specified user has changed the floating IP address of the Chassis Management Module external network interface to the specified value.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Network change (Informational)

SNMP Trap ID
mmTrapNwChangeS

CIM Information
Prefix: CMM **ID:** 0643

User Response
Information only; no action is required.

- **00017129 : Ethernet [[arg1]] interface is up for the standby Chassis Management Module.**

The Chassis Management Module external Ethernet interface is up for the standby Chassis Management Module.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0655

User Response
Information only; no action is required.

- **0001712A : Ethernet [[arg1]] interface is down for the standby Chassis Management Module.**

The Chassis Management Module external Ethernet interface is down for the standby Chassis Management Module. Devices internal to the chassis on the management network, such as system-management processors and the Flex System Manager management module, will also lose network connectivity.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0656

User Response
Complete the following steps until the problem is solved:

1. Make sure that the external Ethernet cable is connected at both ends.
2. Make sure that the cable is working:
   a. Swap both ends of the cable.
   b. Make sure that the link LED on the RJ-45 connector is lit on the Chassis Management Module (CMM) and on the network device to which the CMM is attached.
3. Make sure that the network switch has power.
4. Make sure that the network infrastructure is operational.

- **00017130 : Ethernet host name=[arg1], IP=[arg2], GW=[arg3], Mask=[arg4] has been removed.**

An IPv4 address has been removed from the list of addresses that the Chassis Management Module can respond to.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0775

User Response
Information only; no action is required.

- **00017131 : Ethernet host name changed from [arg1] to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

Ethernet host name changed.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0808

User Response
Information only; no action is required.

- **00017140 : User ID [arg1] at IP [arg2] performed an ACK on alarm ID [arg3].**

  User acknowledged an alarm in the alarm list.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0824

  User Response
  Information only; no action is required.

- **00017141 : User ID [arg1] at IP [arg2] performed an UNACK on alarm ID [arg3].**

  User unacknowledged an alarm in the alarm list.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0825

  User Response
  Information only; no action is required.

- **00017142 : User ID [arg1] at IP [arg2] performed a CLEAR on alarm ID [arg3].**

  User cleared an alarm in the alarm list.

  Severity
  Informational

  Serviceable

No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0826

User Response
Information only; no action is required.

- **00017143 : User ID [arg1] at IP [arg2] entered alarm ID [arg3] which could not be found in alarm list.**

  User entered and alarm ID that was not found in the alarm list.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0827

  User Response
  Information only; no action is required.

- **00017150 : [arg1].**

  The user created software event with a given severity and text.

  Severity
  Error

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0864

  User Response
  Information only; no action is required.

- **00017151 : [arg1].**

  The user created software event with a given severity and text.

  Severity
  Warning

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0865

  User Response
  Information only; no action is required.
- **00017152 : [arg1].**

  The user created software event with a given severity and text.

  Severity
  Warning

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0866

  User Response
  Information only; no action is required.
- **00017200 : Virtual reseat of I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has performed a virtual reseat to reset the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0349

User Response
Information only; no action is required.

- **00017310 : The CIM-XML interface is up.**

  The CIM-XML application is available to subscribers and external interfaces.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0108

  User Response
  Information only; no action is required.

- **0001D400 : Chassis Management Module [arg1] is over recommended temperature.**

  The Chassis Management Module temperature has exceeded the recommended range. The cooling capacity of the chassis has been set to the maximum, and the fan modules are running at full speed.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0224

  User Response
  Complete the following steps until the problem is solved:

  1. Check the ambient room temperature to ensure that the room is not too hot.
  2. Check for any blockage on or near the ventilation holes on the chassis. Remove any blockages that you find.

3. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that nothing is covering the bays. Empty bays can cause a reduction in airflow to the devices in the chassis.
4. Make sure that enough fan modules are installed to sufficiently cool the devices in the chassis. See the chassis documentation to determine how many fan modules are required.

- **0001D502 : Chassis [arg1] ambient temperature is over recommended temperature.**

  The chassis ambient temperature that is readable from the rear LED card has exceeded the recommended range. The cooling capacity of the chassis has been set to the maximum, and the fan modules are running at full speed.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0168

  User Response
  Complete the following steps until the problem is solved:

  1. Check the ambient room temperature to ensure that the room is not too hot.
  2. Check for any blockage on or near the ventilation holes on the chassis. Remove any blockages that you find.
  3. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that nothing is covering the bays. Empty bays can cause a reduction in airflow to the devices in the chassis.
  4. Make sure that enough fan modules are installed to sufficiently cool the devices in the chassis. See the chassis documentation to determine how many fan modules are required.

- **0001D600 : Chassis ambient temperature is out of range.**

  The ambient temperature of the chassis is outside of the operational range.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0823

User Response

Complete the following steps until the problem is solved:

1. Check the ambient room temperature to ensure that the room is not too hot.
2. Check for any blockage on or near the ventilation holes on the chassis. Remove any blockages that you find.
3. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that nothing is covering the bays. Empty bays can cause a reduction in airflow to the devices in the chassis.
4. Make sure that enough fan modules are installed to sufficiently cool the devices in the chassis. See the chassis documentation to determine how many fan modules are required.

- **00022003 : Primary Chassis Management Module real-time clock failed.**

The primary Chassis Management Module (CMM) real-time clock has failed during the built-in self test (BIST). Time stamps in the event log might not be accurate.

Severity

Error

Serviceable

Yes

Automatically notify support

Yes

Alert Category

Chassis/System Management (Critical)

SNMP Trap ID

mmTrapChassisC

CIM Information

Prefix: CMM **ID:** 0589

User Response

Complete the following steps until the problem is solved:

1. Replace the battery in the CMM.
2. Replace the primary CMM.

- **00022008 : Primary Chassis Management Module external Ethernet port failed.**

The Ethernet connection on the primary Chassis Management Module has been broken.

Severity

Error

Serviceable

Yes

Automatically notify support

No

Alert Category

Chassis/System Management (Critical)

SNMP Trap ID

mmTrapChassisC

CIM Information

Prefix: CMM **ID:** 0591

User Response

Make sure that the Chassis Management Module is connected to the network and the cable and external switch are functional.

- **0002200A : Primary Chassis Management Module internal Ethernet logic failed.**

  Ethernet port 0 on the primary Chassis Management Module has failed.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0593

  User Response
  Replace the Chassis Management Module.

- **00022015 : Standby Chassis Management Module real-time clock failed.**

  The standby Chassis Management Module (CMM) real-time clock failed during the built-in self-test (BIST).

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0594

  User Response
  Complete the following steps until the problem is solved:

  1. Replace the battery in the standby CMM.
  2. Replace the standby CMM.

- **00022016 : Standby Chassis Management Module local management bus failed.**

  An internal management bus on the standby Chassis Management Module has failed.

  Severity
  Error

  Serviceable
  Yes

Automatically notify support
Yes

Alert Category
Chassis/System Management (Critical)

SNMP Trap ID
mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0595

User Response
Replace the Chassis Management Module.

- **00022019 : Standby Chassis Management Module internal I/O logic failure.**

  The internal I/O logic on the standby Chassis Management Module failed during the built-in self-test (BIST).

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0600

  User Response
  Replace the standby Chassis Management Module.

- **0002201C : Standby Chassis Management Module external Ethernet port failed.**

  The Ethernet connection on the standby Chassis Management Module has been broken.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0596

  User Response
  Make sure that the Chassis Management Module is connected to the network and the cable and external switch are functional.

- **0002201D : Standby Chassis Management Module internal Ethernet logic failed.**

  Ethernet port 0 on the standby Chassis Management Module has failed.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0597

  User Response
  Replace the standby Chassis Management Module.
- **0002201E : Standby Chassis Management Module communication is offline.**

  The primary Chassis Management Module (CMM) cannot communicate with the standby CMM. Logs and setting changes will not be mirrored to the standby CMM.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0812

  User Response
  The problem might correct itself within approximately 2 minutes. If it does not correct itself, complete the following steps until the problem is solved:

  1. Perform a service-level reset of the standby CMM, to restart the standby CMM. If the problem has not corrected itself, this event will appear again in the log within approximately 5 minutes.
  2. Save the configuration from the primary CMM to a file, and restart the primary CMM. This will probably cause a failover to the standby CMM, and the standby CMM will become the primary CMM. If this event does not appear again in the log within approximately 5 minutes, the problem is now corrected. If the CMM configuration was changed while the primary CMM was unable to communicate with the standby CMM, apply the saved configuration to the current primary CMM.
  3. Replace the current standby CMM. If this event does not appear again in the log after approximately 5 minutes, the problem is now corrected. To prevent failovers that result from minor problems that are related to configuration differences between the CMMs that are not related to CMM hardware failures, consider temporarily removing the standby CMM until you can

replace it. If the configurations on the primary CMM and standby CMM are the same, you can disregard this event until you are able to replace the CMM. After you replace the standby CMM, if the problem was in the standby CMM, the new standby CMM will automatically synchronize the firmware and configuration data with the primary CMM. (Older log entries will not be synchronized, but new log entries will start being synchronized.)

4. Save the configuration from the current primary CMM to a file (the same configuration that you saved in step 2), and replace the current primary CMM. The current standby CMM automatically becomes the primary CMM. If necessary, apply the saved configuration to what is now the primary CMM.

- **0002205A : Primary Chassis Management Module internal I/O logic failure.**

  The internal I/O logic on the primary Chassis Management Module failed during the built-in self-test (BIST).

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0599

  User Response
  Replace the Chassis Management Module.

- **00026801 : Fan module [arg1] has failed.**

  The specified fan module is no longer operating.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Critical)

  SNMP Trap ID
  mmTrapFanC

  CIM Information
  Prefix: CMM **ID:** 0397

  User Response
  Replace the fan module.

- **00026802 : Fan module [arg1] has failed.**

  The specified fan module is no longer operating.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Cooling Devices (Critical)

SNMP Trap ID
mmTrapFanC

CIM Information
Prefix: CMM **ID:** 0397

User Response
Replace the fan module.

- **00026803 : Fan module [arg1] has failed.**

  The specified fan module is no longer operating.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Critical)

  SNMP Trap ID
  mmTrapFanC

  CIM Information
  Prefix: CMM **ID:** 0397

  User Response
  Replace the fan module.

- **00026804 : Fan module [arg1] has failed.**

  The specified fan module is no longer operating.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Critical)

  SNMP Trap ID
  mmTrapFanC

  CIM Information

Prefix: CMM **ID:** 0397

User Response
Replace the fan module.

- **00026805 : Fan module [arg1] has failed.**

  The specified fan module is no longer operating.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Critical)

  SNMP Trap ID
  mmTrapFanC

  CIM Information
  Prefix: CMM **ID:** 0397

  User Response
  Replace the fan module.

- **00026806 : Fan module [arg1] has failed.**

  The specified fan module is no longer operating.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Critical)

  SNMP Trap ID
  mmTrapFanC

  CIM Information
  Prefix: CMM **ID:** 0397

  User Response
  Replace the fan module.

- **00026807 : Fan module [arg1] has failed.**

  The specified fan module is no longer operating.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

Alert Category
Cooling Devices (Critical)

SNMP Trap ID
mmTrapFanC

CIM Information
Prefix: CMM **ID:** 0397

User Response
Replace the fan module.

- **00026808 : Fan module [arg1] has failed.**

  The specified fan module is no longer operating.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Critical)

  SNMP Trap ID
  mmTrapFanC

  CIM Information
  Prefix: CMM **ID:** 0397

  User Response
  Replace the fan module.

- **00026809 : Fan module [arg1] has failed.**

  The specified fan module is no longer operating.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Critical)

  SNMP Trap ID
  mmTrapFanC

  CIM Information
  Prefix: CMM **ID:** 0397

  User Response
  Replace the fan module.

- **0002680A : Fan module [arg1] has failed.**

  The specified fan module is no longer operating.

  Severity

Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Cooling Devices (Critical)

SNMP Trap ID
mmTrapFanC

CIM Information
Prefix: CMM **ID:** 0397

User Response
Replace the fan module.

- **00038101 : Cooling zone [arg1] might not have adequate cooling.**

  One or more fan modules or fan logic modules in the specified cooling zone have failed or have been removed. If additional fan modules or fan logic modules fail or are removed, chassis devices might shut down or throttle because of excessive temperatures. Consider moving applications that are running on nodes in the specified cooling zone to nodes in another cooling zone to ensure the availability of those applications. Note that the fan modules might run faster than normal to compensate for reduced cooling.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0009

  User Response
  Complete the following steps until the problem is solved:

  1. If you removed a fan module, replace the fan module. Fan module presence can be verified by checking the chassis hardware topology.
  2. If you removed a fan logic module, replace the fan logic module. Fan logic module presence can be verified by checking the chassis hardware topology
  3. Look in the Chassis Management Module event log for errors related to fan module or fan logic module events, and solve them.

- **00038102 : Cooling zone [arg1] might not have adequate cooling.**

  One or more fan modules or fan logic modules in the specified cooling zone have failed or have been removed. If additional fan modules or fan logic modules fail or are removed, chassis devices might shut down or throttle because of excessive temperatures. Consider moving applications that are running on nodes in the specified cooling zone to nodes in another cooling zone to ensure the availability of those applications. Note that the fan modules might run faster than normal to compensate for reduced cooling.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0009

User Response
Complete the following steps until the problem is solved:

1. If you removed a fan module, replace the fan module. Fan module presence can be verified by checking the chassis hardware topology.
2. If you removed a fan logic module, replace the fan logic module. Fan logic module presence can be verified by checking the chassis hardware topology
3. Look in the Chassis Management Module event log for errors related to fan module or fan logic module events, and solve them.

- **00038103 : Cooling zone [arg1] might not have adequate cooling.**

One or more fan modules or fan logic modules in the specified cooling zone have failed or have been removed. If additional fan modules or fan logic modules fail or are removed, chassis devices might shut down or throttle because of excessive temperatures. Consider moving applications that are running on nodes in the specified cooling zone to nodes in another cooling zone to ensure the availability of those applications. Note that the fan modules might run faster than normal to compensate for reduced cooling.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0009

User Response
Complete the following steps until the problem is solved:

1. If you removed a fan module, replace the fan module. Fan module presence can be verified by checking the chassis hardware topology.
2. If you removed a fan logic module, replace the fan logic module. Fan logic module presence can be verified by checking the chassis hardware topology

3. Look in the Chassis Management Module event log for errors related to fan module or fan logic module events, and solve them.

- **00038104 : Cooling zone [arg1] might not have adequate cooling.**

  One or more fan modules or fan logic modules in the specified cooling zone have failed or have been removed. If additional fan modules or fan logic modules fail or are removed, chassis devices might shut down or throttle because of excessive temperatures. Consider moving applications that are running on nodes in the specified cooling zone to nodes in another cooling zone to ensure the availability of those applications. Note that the fan modules might run faster than normal to compensate for reduced cooling.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0009

  User Response
  Complete the following steps until the problem is solved:

  1. If you removed a fan module, replace the fan module. Fan module presence can be verified by checking the chassis hardware topology.
  2. If you removed a fan logic module, replace the fan logic module. Fan logic module presence can be verified by checking the chassis hardware topology
  3. Look in the Chassis Management Module event log for errors related to fan module or fan logic module events, and solve them.

- **00038201 : Power supply [arg1] transient reading overvoltage.**

  The specified power supply encountered an intermittent over-voltage error.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Warning)

  SNMP Trap ID
  mmTrapPowerN

  CIM Information
  Prefix: CMM **ID:** 0032

  User Response
  At the next scheduled maintenance opportunity, replace the specified power supply.

- **00038202 : Power supply [arg1] transient reading overvoltage.**

The specified power supply encountered an intermittent over-voltage error.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Power Modules (Warning)

SNMP Trap ID
mmTrapPowerN

CIM Information
Prefix: CMM **ID:** 0032

User Response
At the next scheduled maintenance opportunity, replace the specified power supply.

- **00038203 : Power supply [arg1] transient reading overvoltage.**

The specified power supply encountered an intermittent over-voltage error.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Power Modules (Warning)

SNMP Trap ID
mmTrapPowerN

CIM Information
Prefix: CMM **ID:** 0032

User Response
At the next scheduled maintenance opportunity, replace the specified power supply.

- **00038204 : Power supply [arg1] transient reading overvoltage.**

The specified power supply encountered an intermittent over-voltage error.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Power Modules (Warning)

SNMP Trap ID
mmTrapPowerN

CIM Information
Prefix: CMM **ID:** 0032

User Response
At the next scheduled maintenance opportunity, replace the specified power supply.

- **00038205 : Power supply [arg1] transient reading overvoltage.**

The specified power supply encountered an intermittent over-voltage error.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Power Modules (Warning)

SNMP Trap ID
mmTrapPowerN

CIM Information
Prefix: CMM **ID:** 0032

User Response
At the next scheduled maintenance opportunity, replace the specified power supply.

- **00038206 : Power supply [arg1] transient reading overvoltage.**

The specified power supply encountered an intermittent over-voltage error.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Power Modules (Warning)

SNMP Trap ID
mmTrapPowerN

CIM Information
Prefix: CMM **ID:** 0032

User Response
At the next scheduled maintenance opportunity, replace the specified power supply.

- **00038301 : Power supply [arg1] transient reading undervoltage.**

The specified power supply encountered an intermittent under-voltage error.

Severity
Warning

Serviceable
Yes

Automatically notify support

Yes

Alert Category
Power Modules (Warning)

SNMP Trap ID
mmTrapPowerN

CIM Information
Prefix: CMM **ID:** 0033

User Response
At the next scheduled maintenance opportunity, replace the specified power supply.

- **00038302 : Power supply [arg1] transient reading undervoltage.**

The specified power supply encountered an intermittent under-voltage error.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Power Modules (Warning)

SNMP Trap ID
mmTrapPowerN

CIM Information
Prefix: CMM **ID:** 0033

User Response
At the next scheduled maintenance opportunity, replace the specified power supply.

- **00038303 : Power supply [arg1] transient reading undervoltage.**

The specified power supply encountered an intermittent under-voltage error.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Power Modules (Warning)

SNMP Trap ID
mmTrapPowerN

CIM Information
Prefix: CMM **ID:** 0033

User Response
At the next scheduled maintenance opportunity, replace the specified power supply.

- **00038304 : Power supply [arg1] transient reading undervoltage.**

The specified power supply encountered an intermittent under-voltage error.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Power Modules (Warning)

SNMP Trap ID
mmTrapPowerN

CIM Information
Prefix: CMM **ID:** 0033

User Response
At the next scheduled maintenance opportunity, replace the specified power supply.

- **00038305 : Power supply [arg1] transient reading undervoltage.**

The specified power supply encountered an intermittent under-voltage error.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Power Modules (Warning)

SNMP Trap ID
mmTrapPowerN

CIM Information
Prefix: CMM **ID:** 0033

User Response
At the next scheduled maintenance opportunity, replace the specified power supply.

- **00038306 : Power supply [arg1] transient reading undervoltage.**

The specified power supply encountered an intermittent under-voltage error.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Power Modules (Warning)

SNMP Trap ID
mmTrapPowerN

CIM Information

Prefix: CMM **ID:** 0033

User Response
At the next scheduled maintenance opportunity, replace the specified power supply.

- **00038401 : Power supply [arg1] transient reading overcurrent.**

The specified power supply encountered an intermittent over-current error.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Power Modules (Warning)

SNMP Trap ID
mmTrapPowerN

CIM Information
Prefix: CMM **ID:** 0034

User Response
At the next scheduled maintenance opportunity, replace the specified power supply.

- **00038402 : Power supply [arg1] transient reading overcurrent.**

The specified power supply encountered an intermittent over-current error.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Power Modules (Warning)

SNMP Trap ID
mmTrapPowerN

CIM Information
Prefix: CMM **ID:** 0034

User Response
At the next scheduled maintenance opportunity, replace the specified power supply.

- **00038403 : Power supply [arg1] transient reading overcurrent.**

The specified power supply encountered an intermittent over-current error.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Power Modules (Warning)

SNMP Trap ID
mmTrapPowerN

CIM Information
Prefix: CMM **ID:** 0034

User Response
At the next scheduled maintenance opportunity, replace the specified power supply.

- **00038404 : Power supply [arg1] transient reading overcurrent.**

The specified power supply encountered an intermittent over-current error.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Power Modules (Warning)

SNMP Trap ID
mmTrapPowerN

CIM Information
Prefix: CMM **ID:** 0034

User Response
At the next scheduled maintenance opportunity, replace the specified power supply.

- **00038405 : Power supply [arg1] transient reading overcurrent.**

The specified power supply encountered an intermittent over-current error.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Power Modules (Warning)

SNMP Trap ID
mmTrapPowerN

CIM Information
Prefix: CMM **ID:** 0034

User Response
At the next scheduled maintenance opportunity, replace the specified power supply.

- **00038406 : Power supply [arg1] transient reading overcurrent.**

The specified power supply encountered an intermittent over-current error.

Severity

Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Power Modules (Warning)

SNMP Trap ID
mmTrapPowerN

CIM Information
Prefix: CMM **ID:** 0034

User Response
At the next scheduled maintenance opportunity, replace the specified power supply.

- **00038501 : Power supply [arg1] power meter is offline.**

The specified power supply is not providing power-metering values. The power supply is still providing power, provided that no power-supply fault for the specified power supply is reported in the Chassis Management Module event log. However, any power-management applications might not receive accurate information.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Power Modules (Warning)

SNMP Trap ID
mmTrapPowerN

CIM Information
Prefix: CMM **ID:** 0035

User Response
At the next scheduled maintenance opportunity, replace the specified power supply.

- **00038502 : Power supply [arg1] power meter is offline.**

The specified power supply is not providing power-metering values. The power supply is still providing power, provided that no power-supply fault for the specified power supply is reported in the Chassis Management Module event log. However, any power-management applications might not receive accurate information.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category

Power Modules (Warning)

SNMP Trap ID
mmTrapPowerN

CIM Information
Prefix: CMM **ID:** 0035

User Response
At the next scheduled maintenance opportunity, replace the specified power supply.

- **00038503 : Power supply [arg1] power meter is offline.**

The specified power supply is not providing power-metering values. The power supply is still providing power, provided that no power-supply fault for the specified power supply is reported in the Chassis Management Module event log. However, any power-management applications might not receive accurate information.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Power Modules (Warning)

SNMP Trap ID
mmTrapPowerN

CIM Information
Prefix: CMM **ID:** 0035

User Response
At the next scheduled maintenance opportunity, replace the specified power supply.

- **00038504 : Power supply [arg1] power meter is offline.**

The specified power supply is not providing power-metering values. The power supply is still providing power, provided that no power-supply fault for the specified power supply is reported in the Chassis Management Module event log. However, any power-management applications might not receive accurate information.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Power Modules (Warning)

SNMP Trap ID
mmTrapPowerN

CIM Information
Prefix: CMM **ID:** 0035

User Response

At the next scheduled maintenance opportunity, replace the specified power supply.

- **00038505 : Power supply [arg1] power meter is offline.**

  The specified power supply is not providing power-metering values. The power supply is still providing power, provided that no power-supply fault for the specified power supply is reported in the Chassis Management Module event log. However, any power-management applications might not receive accurate information.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Warning)

  SNMP Trap ID
  mmTrapPowerN

  CIM Information
  Prefix: CMM **ID:** 0035

  User Response
  At the next scheduled maintenance opportunity, replace the specified power supply.

- **00038506 : Power supply [arg1] power meter is offline.**

  The specified power supply is not providing power-metering values. The power supply is still providing power, provided that no power-supply fault for the specified power supply is reported in the Chassis Management Module event log. However, any power-management applications might not receive accurate information.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Warning)

  SNMP Trap ID
  mmTrapPowerN

  CIM Information
  Prefix: CMM **ID:** 0035

  User Response
  At the next scheduled maintenance opportunity, replace the specified power supply.

- **00038601 : Fan module [arg1] VPD is not valid.**

  The vital product data (VPD) of the specified fan module is not valid. VPD includes information such as the serial number and part number to uniquely identify the fan module.

  Severity
  Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Cooling Devices (Warning)

SNMP Trap ID
mmTrapFanN

CIM Information
Prefix: CMM **ID:** 0010

User Response
Replace the fan module.

- **00038602 : Fan module [arg1] VPD is not valid.**

  The vital product data (VPD) of the specified fan module is not valid. VPD includes information such as the serial number and part number to uniquely identify the fan module.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Warning)

  SNMP Trap ID
  mmTrapFanN

  CIM Information
  Prefix: CMM **ID:** 0010

  User Response
  Replace the fan module.

- **00038603 : Fan module [arg1] VPD is not valid.**

  The vital product data (VPD) of the specified fan module is not valid. VPD includes information such as the serial number and part number to uniquely identify the fan module.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Warning)

  SNMP Trap ID
  mmTrapFanN

  CIM Information
  Prefix: CMM **ID:** 0010

User Response
Replace the fan module.

- **00038604 : Fan module [arg1] VPD is not valid.**

  The vital product data (VPD) of the specified fan module is not valid. VPD includes information such as the serial number and part number to uniquely identify the fan module.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Warning)

  SNMP Trap ID
  mmTrapFanN

  CIM Information
  Prefix: CMM **ID:** 0010

  User Response
  Replace the fan module.

- **00038605 : Fan module [arg1] VPD is not valid.**

  The vital product data (VPD) of the specified fan module is not valid. VPD includes information such as the serial number and part number to uniquely identify the fan module.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Warning)

  SNMP Trap ID
  mmTrapFanN

  CIM Information
  Prefix: CMM **ID:** 0010

  User Response
  Replace the fan module.

- **00038606 : Fan module [arg1] VPD is not valid.**

  The vital product data (VPD) of the specified fan module is not valid. VPD includes information such as the serial number and part number to uniquely identify the fan module.

  Severity
  Warning

  Serviceable
  Yes

Automatically notify support
Yes

Alert Category
Cooling Devices (Warning)

SNMP Trap ID
mmTrapFanN

CIM Information
Prefix: CMM **ID:** 0010

User Response
Replace the fan module.

- **00038607 : Fan module [arg1] VPD is not valid.**

  The vital product data (VPD) of the specified fan module is not valid. VPD includes information such as the serial number and part number to uniquely identify the fan module.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Warning)

  SNMP Trap ID
  mmTrapFanN

  CIM Information
  Prefix: CMM **ID:** 0010

  User Response
  Replace the fan module.

- **00038608 : Fan module [arg1] VPD is not valid.**

  The vital product data (VPD) of the specified fan module is not valid. VPD includes information such as the serial number and part number to uniquely identify the fan module.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Warning)

  SNMP Trap ID
  mmTrapFanN

  CIM Information
  Prefix: CMM **ID:** 0010

  User Response
  Replace the fan module.

- **00038609 : Fan module [arg1] VPD is not valid.**

  The vital product data (VPD) of the specified fan module is not valid. VPD includes information such as the serial number and part number to uniquely identify the fan module.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Warning)

  SNMP Trap ID
  mmTrapFanN

  CIM Information
  Prefix: CMM **ID:** 0010

  User Response
  Replace the fan module.
- **0003860A : Fan module [arg1] VPD is not valid.**

  The vital product data (VPD) of the specified fan module is not valid. VPD includes information such as the serial number and part number to uniquely identify the fan module.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Warning)

  SNMP Trap ID
  mmTrapFanN

  CIM Information
  Prefix: CMM **ID:** 0010

  User Response
  Replace the fan module.
- **00038701 : Fan logic module [arg1] VPD is not valid.**

  The vital product data (VPD) of the specified fan logic module is not valid. VPD contains information such as the serial number and part number to uniquely identify the fan logic module.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

Alert Category
Cooling Devices (Warning)

SNMP Trap ID
mmTrapFanN

CIM Information
Prefix: CMM **ID:** 0120

User Response
Replace the fan logic module.

- **00038702 : Fan logic module [arg1] VPD is not valid.**

  The vital product data (VPD) of the specified fan logic module is not valid. VPD contains information such as the serial number and part number to uniquely identify the fan logic module.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Warning)

  SNMP Trap ID
  mmTrapFanN

  CIM Information
  Prefix: CMM **ID:** 0120

  User Response
  Replace the fan logic module.

- **00038901 : The [arg1] log has been initialized.**

  The Chassis Management Module (CMM) log specified in [arg1] has been automatically cleared. The specified log can be "system" or "audit". The CMM will automatically clear the logs if a user has restored the default configuration to the CMM and did not select to preserve the logs. The logs could also be cleared if corruption is detected by the CMM firmware.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0005

  User Response
  Information only; no action is required.

- **00038A01 : Power supply [arg1] VPD is not valid.**

  The vital product data (VPD) of the specified power supply is not valid. VPD includes information such as the serial number and part number to uniquely identify the power supply.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Warning)

  SNMP Trap ID
  mmTrapPowerN

  CIM Information
  Prefix: CMM **ID:** 0045

  User Response
  Replace the power supply.
- **00038A02 : Power supply [arg1] VPD is not valid.**

  The vital product data (VPD) of the specified power supply is not valid. VPD includes information such as the serial number and part number to uniquely identify the power supply.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Warning)

  SNMP Trap ID
  mmTrapPowerN

  CIM Information
  Prefix: CMM **ID:** 0045

  User Response
  Replace the power supply.
- **00038A03 : Power supply [arg1] VPD is not valid.**

  The vital product data (VPD) of the specified power supply is not valid. VPD includes information such as the serial number and part number to uniquely identify the power supply.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

Alert Category
Power Modules (Warning)

SNMP Trap ID
mmTrapPowerN

CIM Information
Prefix: CMM **ID:** 0045

User Response
Replace the power supply.

- **00038A04 : Power supply [arg1] VPD is not valid.**

  The vital product data (VPD) of the specified power supply is not valid. VPD includes information such as the serial number and part number to uniquely identify the power supply.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Warning)

  SNMP Trap ID
  mmTrapPowerN

  CIM Information
  Prefix: CMM **ID:** 0045

  User Response
  Replace the power supply.

- **00038A05 : Power supply [arg1] VPD is not valid.**

  The vital product data (VPD) of the specified power supply is not valid. VPD includes information such as the serial number and part number to uniquely identify the power supply.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Warning)

  SNMP Trap ID
  mmTrapPowerN

  CIM Information
  Prefix: CMM **ID:** 0045

  User Response
  Replace the power supply.

- **00038A06 : Power supply [arg1] VPD is not valid.**

The vital product data (VPD) of the specified power supply is not valid. VPD includes information such as the serial number and part number to uniquely identify the power supply.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Power Modules (Warning)

SNMP Trap ID
mmTrapPowerN

CIM Information
Prefix: CMM **ID:** 0045

User Response
Replace the power supply.

- **00038B01 : Adequate cooling has been restored in cooling zone [arg1].**

The airflow is now adequate to cool devices in the cooling zone.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0016

User Response
Information only; no action is required.

- **00038B02 : Adequate cooling has been restored in cooling zone [arg1].**

The airflow is now adequate to cool devices in the cooling zone.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID

mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0016

User Response
Information only; no action is required.

- **00038B03 : Adequate cooling has been restored in cooling zone [arg1].**

  The airflow is now adequate to cool devices in the cooling zone.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0016

  User Response
  Information only; no action is required.

- **00038B04 : Adequate cooling has been restored in cooling zone [arg1].**

  The airflow is now adequate to cool devices in the cooling zone.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0016

  User Response
  Information only; no action is required.

- **00038C01 : I/O module [arg1] is within the recommended temperature range.**

  The temperature of the specified I/O module is within the recommended range. This event occurs when the temperatures of I/O modules have exceeded the normal operating range but are now back within the recommended range.

  Severity
  Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0048

User Response
Information only; no action is required.

- **00038C02 : I/O module [arg1] is within the recommended temperature range.**

  The temperature of the specified I/O module is within the recommended range. This event occurs when the temperatures of I/O modules have exceeded the normal operating range but are now back within the recommended range.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0048

  User Response
  Information only; no action is required.

- **00038C03 : I/O module [arg1] is within the recommended temperature range.**

  The temperature of the specified I/O module is within the recommended range. This event occurs when the temperatures of I/O modules have exceeded the normal operating range but are now back within the recommended range.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0048

User Response
Information only; no action is required.

- **00038C04 : I/O module [arg1] is within the recommended temperature range.**

  The temperature of the specified I/O module is within the recommended range. This event occurs when the temperatures of I/O modules have exceeded the normal operating range but are now back within the recommended range.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0048

  User Response
  Information only; no action is required.

- **00038D01 : Power supply [arg1] temperature is normal.**

  The power supply was exceeding temperature thresholds but is now running within normal temperatures.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Power Modules (Informational)

  SNMP Trap ID
  mmTrapPowerS

  CIM Information
  Prefix: CMM **ID:** 0025

  User Response
  Information only; no action is required.

- **00038D02 : Power supply [arg1] temperature is normal.**

  The power supply was exceeding temperature thresholds but is now running within normal temperatures.

  Severity
  Informational

  Serviceable

No

Automatically notify support
No

Alert Category
Power Modules (Informational)

SNMP Trap ID
mmTrapPowerS

CIM Information
Prefix: CMM **ID:** 0025

User Response
Information only; no action is required.

- **00038D03 : Power supply [arg1] temperature is normal.**

The power supply was exceeding temperature thresholds but is now running within normal temperatures.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Power Modules (Informational)

SNMP Trap ID
mmTrapPowerS

CIM Information
Prefix: CMM **ID:** 0025

User Response
Information only; no action is required.

- **00038D04 : Power supply [arg1] temperature is normal.**

The power supply was exceeding temperature thresholds but is now running within normal temperatures.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Power Modules (Informational)

SNMP Trap ID
mmTrapPowerS

CIM Information
Prefix: CMM **ID:** 0025

User Response
Information only; no action is required.

- **00038D05 : Power supply [arg1] temperature is normal.**

  The power supply was exceeding temperature thresholds but is now running within normal temperatures.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Power Modules (Informational)

  SNMP Trap ID
  mmTrapPowerS

  CIM Information
  Prefix: CMM **ID:** 0025

  User Response
  Information only; no action is required.
- **00038D06 : Power supply [arg1] temperature is normal.**

  The power supply was exceeding temperature thresholds but is now running within normal temperatures.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Power Modules (Informational)

  SNMP Trap ID
  mmTrapPowerS

  CIM Information
  Prefix: CMM **ID:** 0025

  User Response
  Information only; no action is required.
- **00038E02 : Secure CIM-XML port number changed from [arg1] to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The secure CIM-XML port number has been changed.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0090

User Response
Information only; no action is required.

- **00038E05 : The chassis name was updated to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the chassis name.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0112

  User Response
  Information only; no action is required.

- **00038E06 : The chassis room location was updated to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the chassis room location identification.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0113

  User Response
  Information only; no action is required.

- **00038E07 : The chassis rack location was updated to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the chassis rack location identification.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0114

User Response
Information only; no action is required.

- **00038E08 : The chassis unit location was updated to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the chassis rack unit identification, which counts the number of units from the bottom of the rack to the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0115

  User Response
  Information only; no action is required.

- **00038F01 : Internal proprietary management protocol between I/O module [arg1] and CMM is offline.**

  The Chassis Management Module (CMM) cannot communicate with the specified I/O module. The I/O module might be operating normally, but the CMM cannot detect whether there are problems with the specified device. This is an internal Ethernet issue for advanced communication. The I2C interface is independent.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

Alert Category
I/O Modules (Warning)

SNMP Trap ID
mmTrapION

CIM Information
Prefix: CMM **ID:** 0096

User Response
Temporarily disable all communication between the nodes and the specified I/O module in the chassis to reduce interruptions to the services that the nodes provide. Perform a service-level reset of the I/O module, which restarts the I/O module. If the service-level reset does not correct the problem, replace the I/O module.

- **00038F02 : Internal proprietary management protocol between I/O module [arg1] and CMM is offline.**

  The Chassis Management Module (CMM) cannot communicate with the specified I/O module. The I/O module might be operating normally, but the CMM cannot detect whether there are problems with the specified device. This is an internal Ethernet issue for advanced communication. The I2C interface is independent.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  I/O Modules (Warning)

  SNMP Trap ID
  mmTrapION

  CIM Information
  Prefix: CMM **ID:** 0096

  User Response
  Temporarily disable all communication between the nodes and the specified I/O module in the chassis to reduce interruptions to the services that the nodes provide. Perform a service-level reset of the I/O module, which restarts the I/O module. If the service-level reset does not correct the problem, replace the I/O module.

- **00038F03 : Internal proprietary management protocol between I/O module [arg1] and CMM is offline.**

  The Chassis Management Module (CMM) cannot communicate with the specified I/O module. The I/O module might be operating normally, but the CMM cannot detect whether there are problems with the specified device. This is an internal Ethernet issue for advanced communication. The I2C interface is independent.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

Alert Category
I/O Modules (Warning)

SNMP Trap ID
mmTrapION

CIM Information
Prefix: CMM **ID:** 0096

User Response
Temporarily disable all communication between the nodes and the specified I/O module in the chassis to reduce interruptions to the services that the nodes provide. Perform a service-level reset of the I/O module, which restarts the I/O module. If the service-level reset does not correct the problem, replace the I/O module.

- **00038F04 : Internal proprietary management protocol between I/O module [arg1] and CMM is offline.**

  The Chassis Management Module (CMM) cannot communicate with the specified I/O module. The I/O module might be operating normally, but the CMM cannot detect whether there are problems with the specified device. This is an internal Ethernet issue for advanced communication. The I2C interface is independent.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  I/O Modules (Warning)

  SNMP Trap ID
  mmTrapION

  CIM Information
  Prefix: CMM **ID:** 0096

  User Response
  Temporarily disable all communication between the nodes and the specified I/O module in the chassis to reduce interruptions to the services that the nodes provide. Perform a service-level reset of the I/O module, which restarts the I/O module. If the service-level reset does not correct the problem, replace the I/O module.

- **00039081 : The chassis cooling configuration might not be adequate for node [arg1].**

  There might not be enough available cooling in the chassis for the node.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID

mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0056

User Response
Complete the following steps until the problem is solved:

1. Solve any cooling issues that are reported in the logs, such as a failed fan module.
2. If applicable, install additional fan modules.
3. Check the acoustic attenuation setting. You might have to reduce the attenuation level or disable acoustic mode.

- **00039082 : The chassis cooling configuration might not be adequate for node [arg1].**

There might not be enough available cooling in the chassis for the node.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0056

User Response
Complete the following steps until the problem is solved:

1. Solve any cooling issues that are reported in the logs, such as a failed fan module.
2. If applicable, install additional fan modules.
3. Check the acoustic attenuation setting. You might have to reduce the attenuation level or disable acoustic mode.

- **00039083 : The chassis cooling configuration might not be adequate for node [arg1].**

There might not be enough available cooling in the chassis for the node.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0056

User Response
Complete the following steps until the problem is solved:

1. Solve any cooling issues that are reported in the logs, such as a failed fan module.
2. If applicable, install additional fan modules.
3. Check the acoustic attenuation setting. You might have to reduce the attenuation level or disable acoustic mode.

- **00039084 : The chassis cooling configuration might not be adequate for node [arg1].**

  There might not be enough available cooling in the chassis for the node.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0056

  User Response
  Complete the following steps until the problem is solved:

  1. Solve any cooling issues that are reported in the logs, such as a failed fan module.
  2. If applicable, install additional fan modules.
  3. Check the acoustic attenuation setting. You might have to reduce the attenuation level or disable acoustic mode.

- **00039085 : The chassis cooling configuration might not be adequate for node [arg1].**

  There might not be enough available cooling in the chassis for the node.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0056

  User Response
  Complete the following steps until the problem is solved:

  1. Solve any cooling issues that are reported in the logs, such as a failed fan module.

2. If applicable, install additional fan modules.
3. Check the acoustic attenuation setting. You might have to reduce the attenuation level or disable acoustic mode.

- **00039086 : The chassis cooling configuration might not be adequate for node [arg1].**

  There might not be enough available cooling in the chassis for the node.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0056

  User Response
  Complete the following steps until the problem is solved:

  1. Solve any cooling issues that are reported in the logs, such as a failed fan module.
  2. If applicable, install additional fan modules.
  3. Check the acoustic attenuation setting. You might have to reduce the attenuation level or disable acoustic mode.

- **00039087 : The chassis cooling configuration might not be adequate for node [arg1].**

  There might not be enough available cooling in the chassis for the node.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0056

  User Response
  Complete the following steps until the problem is solved:

  1. Solve any cooling issues that are reported in the logs, such as a failed fan module.
  2. If applicable, install additional fan modules.
  3. Check the acoustic attenuation setting. You might have to reduce the attenuation level or disable acoustic mode.

- **00039088 : The chassis cooling configuration might not be adequate for node [arg1].**

  There might not be enough available cooling in the chassis for the node.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0056

  User Response
  Complete the following steps until the problem is solved:

  1. Solve any cooling issues that are reported in the logs, such as a failed fan module.
  2. If applicable, install additional fan modules.
  3. Check the acoustic attenuation setting. You might have to reduce the attenuation level or disable acoustic mode.

- **00039089 : The chassis cooling configuration might not be adequate for node [arg1].**

  There might not be enough available cooling in the chassis for the node.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0056

  User Response
  Complete the following steps until the problem is solved:

  1. Solve any cooling issues that are reported in the logs, such as a failed fan module.
  2. If applicable, install additional fan modules.
  3. Check the acoustic attenuation setting. You might have to reduce the attenuation level or disable acoustic mode.

- **0003908A : The chassis cooling configuration might not be adequate for node [arg1].**

  There might not be enough available cooling in the chassis for the node.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0056

User Response
Complete the following steps until the problem is solved:

1. Solve any cooling issues that are reported in the logs, such as a failed fan module.
2. If applicable, install additional fan modules.
3. Check the acoustic attenuation setting. You might have to reduce the attenuation level or disable acoustic mode.

- **0003908B : The chassis cooling configuration might not be adequate for node [arg1].**

  There might not be enough available cooling in the chassis for the node.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0056

  User Response
  Complete the following steps until the problem is solved:

  1. Solve any cooling issues that are reported in the logs, such as a failed fan module.
  2. If applicable, install additional fan modules.
  3. Check the acoustic attenuation setting. You might have to reduce the attenuation level or disable acoustic mode.

- **0003908C : The chassis cooling configuration might not be adequate for node [arg1].**

  There might not be enough available cooling in the chassis for the node.

  Severity
  Warning

  Serviceable

Yes

Automatically notify support
No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0056

User Response
Complete the following steps until the problem is solved:

1. Solve any cooling issues that are reported in the logs, such as a failed fan module.
2. If applicable, install additional fan modules.
3. Check the acoustic attenuation setting. You might have to reduce the attenuation level or disable acoustic mode.

- **0003908D : The chassis cooling configuration might not be adequate for node [arg1].**

  There might not be enough available cooling in the chassis for the node.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0056

  User Response
  Complete the following steps until the problem is solved:

  1. Solve any cooling issues that are reported in the logs, such as a failed fan module.
  2. If applicable, install additional fan modules.
  3. Check the acoustic attenuation setting. You might have to reduce the attenuation level or disable acoustic mode.

- **0003908E : The chassis cooling configuration might not be adequate for node [arg1].**

  There might not be enough available cooling in the chassis for the node.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0056

User Response
Complete the following steps until the problem is solved:

1. Solve any cooling issues that are reported in the logs, such as a failed fan module.
2. If applicable, install additional fan modules.
3. Check the acoustic attenuation setting. You might have to reduce the attenuation level or disable acoustic mode.

- **00039101 : Node [arg1] cannot power on because of insufficient cooling.**

The specified node cannot power on because no cooling is available for the node.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0253

User Response
Make sure that there is a chassis cooling device in the corresponding cooling zone. For a 2-bay node, cooling devices are required in both cooling zones.

- **00039102 : Node [arg1] cannot power on because of insufficient cooling.**

The specified node cannot power on because no cooling is available for the node.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0253

User Response
Make sure that there is a chassis cooling device in the corresponding cooling zone. For a 2-bay node, cooling devices are required in both cooling zones.

- **00039103 : Node [arg1] cannot power on because of insufficient cooling.**

The specified node cannot power on because no cooling is available for the node.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0253

User Response
Make sure that there is a chassis cooling device in the corresponding cooling zone. For a 2-bay node, cooling devices are required in both cooling zones.

- **00039104 : Node [arg1] cannot power on because of insufficient cooling.**

The specified node cannot power on because no cooling is available for the node.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0253

User Response
Make sure that there is a chassis cooling device in the corresponding cooling zone. For a 2-bay node, cooling devices are required in both cooling zones.

- **00039105 : Node [arg1] cannot power on because of insufficient cooling.**

The specified node cannot power on because no cooling is available for the node.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0253

User Response
Make sure that there is a chassis cooling device in the corresponding cooling zone. For a 2-bay node, cooling devices are required in both cooling zones.

- **00039106 : Node [arg1] cannot power on because of insufficient cooling.**

The specified node cannot power on because no cooling is available for the node.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0253

User Response
Make sure that there is a chassis cooling device in the corresponding cooling zone. For a 2-bay node, cooling devices are required in both cooling zones.

- **00039107 : Node [arg1] cannot power on because of insufficient cooling.**

The specified node cannot power on because no cooling is available for the node.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0253

User Response

Make sure that there is a chassis cooling device in the corresponding cooling zone. For a 2-bay node, cooling devices are required in both cooling zones.

- **00039108 : Node [arg1] cannot power on because of insufficient cooling.**

  The specified node cannot power on because no cooling is available for the node.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0253

  User Response
  Make sure that there is a chassis cooling device in the corresponding cooling zone. For a 2-bay node, cooling devices are required in both cooling zones.

- **00039109 : Node [arg1] cannot power on because of insufficient cooling.**

  The specified node cannot power on because no cooling is available for the node.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0253

  User Response
  Make sure that there is a chassis cooling device in the corresponding cooling zone. For a 2-bay node, cooling devices are required in both cooling zones.

- **0003910A : Node [arg1] cannot power on because of insufficient cooling.**

  The specified node cannot power on because no cooling is available for the node.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support

No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0253

User Response
Make sure that there is a chassis cooling device in the corresponding cooling zone. For a 2-bay node, cooling devices are required in both cooling zones.

- **0003910B : Node [arg1] cannot power on because of insufficient cooling.**

  The specified node cannot power on because no cooling is available for the node.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0253

  User Response
  Make sure that there is a chassis cooling device in the corresponding cooling zone. For a 2-bay node, cooling devices are required in both cooling zones.

- **0003910C : Node [arg1] cannot power on because of insufficient cooling.**

  The specified node cannot power on because no cooling is available for the node.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0253

  User Response
  Make sure that there is a chassis cooling device in the corresponding cooling zone. For a 2-bay node, cooling devices are required in both cooling zones.

- **0003910D : Node [arg1] cannot power on because of insufficient cooling.**

  The specified node cannot power on because no cooling is available for the node.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0253

  User Response
  Make sure that there is a chassis cooling device in the corresponding cooling zone. For a 2-bay node, cooling devices are required in both cooling zones.
- **0003910E : Node [arg1] cannot power on because of insufficient cooling.**

  The specified node cannot power on because no cooling is available for the node.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0253

  User Response
  Make sure that there is a chassis cooling device in the corresponding cooling zone. For a 2-bay node, cooling devices are required in both cooling zones.
- **00039201 : Cooling is insufficient for node [arg1] due to cooling mismatch [arg2].**

  There might not be enough available cooling in the chassis for the node.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category

Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0679

User Response
The cooling devices may be of lower capacity, they should be replaced with higher capacity fans.

- **00039202 : Cooling is insufficient for node [arg1] due to cooling mismatch [arg2].**

There might not be enough available cooling in the chassis for the node.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0679

User Response
The cooling devices may be of lower capacity, they should be replaced with higher capacity fans.

- **00039203 : Cooling is insufficient for node [arg1] due to cooling mismatch [arg2].**

There might not be enough available cooling in the chassis for the node.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0679

User Response
The cooling devices may be of lower capacity, they should be replaced with higher capacity fans.

- **00039204 : Cooling is insufficient for node [arg1] due to cooling mismatch [arg2].**

There might not be enough available cooling in the chassis for the node.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0679

User Response
The cooling devices may be of lower capacity, they should be replaced with higher capacity fans.

- **00039205 : Cooling is insufficient for node [arg1] due to cooling mismatch [arg2].**

There might not be enough available cooling in the chassis for the node.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0679

User Response
The cooling devices may be of lower capacity, they should be replaced with higher capacity fans.

- **00039206 : Cooling is insufficient for node [arg1] due to cooling mismatch [arg2].**

There might not be enough available cooling in the chassis for the node.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0679

User Response

The cooling devices may be of lower capacity, they should be replaced with higher capacity fans.

- **00039207 : Cooling is insufficient for node [arg1] due to cooling mismatch [arg2].**

  There might not be enough available cooling in the chassis for the node.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0679

  User Response
  The cooling devices may be of lower capacity, they should be replaced with higher capacity fans.

- **00039208 : Cooling is insufficient for node [arg1] due to cooling mismatch [arg2].**

  There might not be enough available cooling in the chassis for the node.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0679

  User Response
  The cooling devices may be of lower capacity, they should be replaced with higher capacity fans.

- **00039209 : Cooling is insufficient for node [arg1] due to cooling mismatch [arg2].**

  There might not be enough available cooling in the chassis for the node.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0679

User Response
The cooling devices may be of lower capacity, they should be replaced with higher capacity fans.

- **0003920A : Cooling is insufficient for node [arg1] due to cooling mismatch [arg2].**

  There might not be enough available cooling in the chassis for the node.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0679

  User Response
  The cooling devices may be of lower capacity, they should be replaced with higher capacity fans.
- **0003920B : Cooling is insufficient for node [arg1] due to cooling mismatch [arg2].**

  There might not be enough available cooling in the chassis for the node.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0679

  User Response
  The cooling devices may be of lower capacity, they should be replaced with higher capacity fans.
- **0003920C : Cooling is insufficient for node [arg1] due to cooling mismatch [arg2].**

  There might not be enough available cooling in the chassis for the node.

  Severity
  Warning

  Serviceable

Yes

Automatically notify support
No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0679

User Response
The cooling devices may be of lower capacity, they should be replaced with higher capacity fans.

- **0003920D : Cooling is insufficient for node [arg1] due to cooling mismatch [arg2].**

There might not be enough available cooling in the chassis for the node.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0679

User Response
The cooling devices may be of lower capacity, they should be replaced with higher capacity fans.

- **0003920E : Cooling is insufficient for node [arg1] due to cooling mismatch [arg2].**

There might not be enough available cooling in the chassis for the node.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0679

User Response
The cooling devices may be of lower capacity, they should be replaced with higher capacity fans.

- **00039601 : Fan module [arg1] VPD is not available.**

  The vital product data (VPD) of the specified fan module is not available. VPD includes information such as the serial number and part number to uniquely identify the fan module.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Warning)

  SNMP Trap ID
  mmTrapFanN

  CIM Information
  Prefix: CMM **ID:** 0104

  User Response
  Replace the fan module.
- **00039602 : Fan module [arg1] VPD is not available.**

  The vital product data (VPD) of the specified fan module is not available. VPD includes information such as the serial number and part number to uniquely identify the fan module.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Warning)

  SNMP Trap ID
  mmTrapFanN

  CIM Information
  Prefix: CMM **ID:** 0104

  User Response
  Replace the fan module.
- **00039603 : Fan module [arg1] VPD is not available.**

  The vital product data (VPD) of the specified fan module is not available. VPD includes information such as the serial number and part number to uniquely identify the fan module.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

Alert Category
Cooling Devices (Warning)

SNMP Trap ID
mmTrapFanN

CIM Information
Prefix: CMM **ID:** 0104

User Response
Replace the fan module.

- **00039604 : Fan module [arg1] VPD is not available.**

  The vital product data (VPD) of the specified fan module is not available. VPD includes information such as the serial number and part number to uniquely identify the fan module.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Warning)

  SNMP Trap ID
  mmTrapFanN

  CIM Information
  Prefix: CMM **ID:** 0104

  User Response
  Replace the fan module.
- **00039605 : Fan module [arg1] VPD is not available.**

  The vital product data (VPD) of the specified fan module is not available. VPD includes information such as the serial number and part number to uniquely identify the fan module.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Warning)

  SNMP Trap ID
  mmTrapFanN

  CIM Information
  Prefix: CMM **ID:** 0104

  User Response
  Replace the fan module.
- **00039606 : Fan module [arg1] VPD is not available.**

The vital product data (VPD) of the specified fan module is not available. VPD includes information such as the serial number and part number to uniquely identify the fan module.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Cooling Devices (Warning)

SNMP Trap ID
mmTrapFanN

CIM Information
Prefix: CMM **ID:** 0104

User Response
Replace the fan module.

- **00039607 : Fan module [arg1] VPD is not available.**

The vital product data (VPD) of the specified fan module is not available. VPD includes information such as the serial number and part number to uniquely identify the fan module.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Cooling Devices (Warning)

SNMP Trap ID
mmTrapFanN

CIM Information
Prefix: CMM **ID:** 0104

User Response
Replace the fan module.

- **00039608 : Fan module [arg1] VPD is not available.**

The vital product data (VPD) of the specified fan module is not available. VPD includes information such as the serial number and part number to uniquely identify the fan module.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category

Cooling Devices (Warning)

SNMP Trap ID
mmTrapFanN

CIM Information
Prefix: CMM **ID:** 0104

User Response
Replace the fan module.

- **00039609 : Fan module [arg1] VPD is not available.**

  The vital product data (VPD) of the specified fan module is not available. VPD includes information such as the serial number and part number to uniquely identify the fan module.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Warning)

  SNMP Trap ID
  mmTrapFanN

  CIM Information
  Prefix: CMM **ID:** 0104

  User Response
  Replace the fan module.

- **0003960A : Fan module [arg1] VPD is not available.**

  The vital product data (VPD) of the specified fan module is not available. VPD includes information such as the serial number and part number to uniquely identify the fan module.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Warning)

  SNMP Trap ID
  mmTrapFanN

  CIM Information
  Prefix: CMM **ID:** 0104

  User Response
  Replace the fan module.

- **00039701 : Fan logic module [arg1] VPD is not available.**

  The vital product data (VPD) of the specified fan logic module is not available. VPD contains information such as the serial number and part number to uniquely identify the fan logic module.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Cooling Devices (Warning)

SNMP Trap ID
mmTrapFanN

CIM Information
Prefix: CMM **ID:** 0105

User Response
Replace the fan logic module.

- **00039702 : Fan logic module [arg1] VPD is not available.**

  The vital product data (VPD) of the specified fan logic module is not available. VPD contains information such as the serial number and part number to uniquely identify the fan logic module.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Warning)

  SNMP Trap ID
  mmTrapFanN

  CIM Information
  Prefix: CMM **ID:** 0105

  User Response
  Replace the fan logic module.

- **00039A01 : Power supply [arg1] VPD is not available.**

  The vital product data (VPD) of the specified power supply is not available. VPD includes information such as the serial number and part number to uniquely identify the power supply.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Warning)

  SNMP Trap ID
  mmTrapPowerN

CIM Information
Prefix: CMM **ID:** 0106

User Response
Replace the power supply.

- **00039A02 : Power supply [arg1] VPD is not available.**

  The vital product data (VPD) of the specified power supply is not available. VPD includes information such as the serial number and part number to uniquely identify the power supply.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Warning)

  SNMP Trap ID
  mmTrapPowerN

  CIM Information
  Prefix: CMM **ID:** 0106

  User Response
  Replace the power supply.

- **00039A03 : Power supply [arg1] VPD is not available.**

  The vital product data (VPD) of the specified power supply is not available. VPD includes information such as the serial number and part number to uniquely identify the power supply.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Warning)

  SNMP Trap ID
  mmTrapPowerN

  CIM Information
  Prefix: CMM **ID:** 0106

  User Response
  Replace the power supply.

- **00039A04 : Power supply [arg1] VPD is not available.**

  The vital product data (VPD) of the specified power supply is not available. VPD includes information such as the serial number and part number to uniquely identify the power supply.

  Severity
  Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Power Modules (Warning)

SNMP Trap ID
mmTrapPowerN

CIM Information
Prefix: CMM **ID:** 0106

User Response
Replace the power supply.

- **00039A05 : Power supply [arg1] VPD is not available.**

  The vital product data (VPD) of the specified power supply is not available. VPD includes information such as the serial number and part number to uniquely identify the power supply.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Warning)

  SNMP Trap ID
  mmTrapPowerN

  CIM Information
  Prefix: CMM **ID:** 0106

  User Response
  Replace the power supply.

- **00039A06 : Power supply [arg1] VPD is not available.**

  The vital product data (VPD) of the specified power supply is not available. VPD includes information such as the serial number and part number to uniquely identify the power supply.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Warning)

  SNMP Trap ID
  mmTrapPowerN

  CIM Information
  Prefix: CMM **ID:** 0106

User Response
Replace the power supply.

- **00039B01 : Fan module [arg1] fan parameter in VPD is not valid.**

  The fan parameter in the vital product data (VPD) of the specified fan module is not valid.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Warning)

  SNMP Trap ID
  mmTrapFanN

  CIM Information
  Prefix: CMM **ID:** 0678

  User Response
  Replace the fan module.
- **00039B02 : Fan module [arg1] fan parameter in VPD is not valid.**

  The fan parameter in the vital product data (VPD) of the specified fan module is not valid.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Warning)

  SNMP Trap ID
  mmTrapFanN

  CIM Information
  Prefix: CMM **ID:** 0678

  User Response
  Replace the fan module.
- **00039B03 : Fan module [arg1] fan parameter in VPD is not valid.**

  The fan parameter in the vital product data (VPD) of the specified fan module is not valid.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category

Cooling Devices (Warning)

SNMP Trap ID
mmTrapFanN

CIM Information
Prefix: CMM **ID:** 0678

User Response
Replace the fan module.

- **00039B04 : Fan module [arg1] fan parameter in VPD is not valid.**

The fan parameter in the vital product data (VPD) of the specified fan module is not valid.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Cooling Devices (Warning)

SNMP Trap ID
mmTrapFanN

CIM Information
Prefix: CMM **ID:** 0678

User Response
Replace the fan module.

- **00039B05 : Fan module [arg1] fan parameter in VPD is not valid.**

The fan parameter in the vital product data (VPD) of the specified fan module is not valid.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Cooling Devices (Warning)

SNMP Trap ID
mmTrapFanN

CIM Information
Prefix: CMM **ID:** 0678

User Response
Replace the fan module.

- **00039B06 : Fan module [arg1] fan parameter in VPD is not valid.**

The fan parameter in the vital product data (VPD) of the specified fan module is not valid.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Cooling Devices (Warning)

SNMP Trap ID
mmTrapFanN

CIM Information
Prefix: CMM **ID:** 0678

User Response
Replace the fan module.

- **00039B07 : Fan module [arg1] fan parameter in VPD is not valid.**

The fan parameter in the vital product data (VPD) of the specified fan module is not valid.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Cooling Devices (Warning)

SNMP Trap ID
mmTrapFanN

CIM Information
Prefix: CMM **ID:** 0678

User Response
Replace the fan module.

- **00039B08 : Fan module [arg1] fan parameter in VPD is not valid.**

The fan parameter in the vital product data (VPD) of the specified fan module is not valid.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Cooling Devices (Warning)

SNMP Trap ID
mmTrapFanN

CIM Information
Prefix: CMM **ID:** 0678

User Response

Replace the fan module.

- **00039B09 : Fan module [arg1] fan parameter in VPD is not valid.**

  The fan parameter in the vital product data (VPD) of the specified fan module is not valid.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Warning)

  SNMP Trap ID
  mmTrapFanN

  CIM Information
  Prefix: CMM **ID:** 0678

  User Response
  Replace the fan module.

- **00039B0A : Fan module [arg1] fan parameter in VPD is not valid.**

  The fan parameter in the vital product data (VPD) of the specified fan module is not valid.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Warning)

  SNMP Trap ID
  mmTrapFanN

  CIM Information
  Prefix: CMM **ID:** 0678

  User Response
  Replace the fan module.

- **000A2101 : Fan logic module [arg1] has failed.**

  A failure has been detected in the fan logic module.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Critical)

SNMP Trap ID
mmTrapFanC

CIM Information
Prefix: CMM **ID:** 0013

User Response
Replace the fan logic module.

- **000A2102 : Fan logic module [arg1] has failed.**

  A failure has been detected in the fan logic module.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Critical)

  SNMP Trap ID
  mmTrapFanC

  CIM Information
  Prefix: CMM **ID:** 0013

  User Response
  Replace the fan logic module.

- **000A2201 : Fan logic module [arg1] is an older revision card (FRU 81Y2912) and needs to be replaced.**

  A Fan Logic Card may experience an early life failure which can result in a communication loss between the CMM and the fans. This will then cause the fans to ramp up to full speed and be noticeably noisier. The system will continue to run. The specified fan logic module needs to be replaced.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Warning)

  SNMP Trap ID
  mmTrapFanN

  CIM Information
  Prefix: CMM **ID:** 0692

  User Response
  Please contact Support and reference ECA-083(System X) or ECA-335(System P).

- **000A2202 : Fan logic module [arg1] is an older revision card (FRU 81Y2912) and needs to be replaced.**

A Fan Logic Card may experience an early life failure which can result in a communication loss between the CMM and the fans. This will then cause the fans to ramp up to full speed and be noticeably noisier. The system will continue to run. The specified fan logic module needs to be replaced.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Cooling Devices (Warning)

SNMP Trap ID
mmTrapFanN

CIM Information
Prefix: CMM **ID:** 0692

User Response
Please contact Support and reference ECA-083(System X) or ECA-335(System P).

- **000A6001 : Fan module [arg1] is operating in a degraded state.**

The specified fan module is not operating at the expected speed.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Cooling Devices (Warning)

SNMP Trap ID
mmTrapFanN

CIM Information
Prefix: CMM **ID:** 0494

User Response
Replace the fan module.

- **000A6002 : Fan module [arg1] is operating in a degraded state.**

The specified fan module is not operating at the expected speed.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Cooling Devices (Warning)

SNMP Trap ID
mmTrapFanN

CIM Information
Prefix: CMM **ID:** 0494

User Response
Replace the fan module.

- **000A6003 : Fan module [arg1] is operating in a degraded state.**

  The specified fan module is not operating at the expected speed.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Warning)

  SNMP Trap ID
  mmTrapFanN

  CIM Information
  Prefix: CMM **ID:** 0494

  User Response
  Replace the fan module.
- **000A6004 : Fan module [arg1] is operating in a degraded state.**

  The specified fan module is not operating at the expected speed.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Warning)

  SNMP Trap ID
  mmTrapFanN

  CIM Information
  Prefix: CMM **ID:** 0494

  User Response
  Replace the fan module.
- **000A6005 : Fan module [arg1] is operating in a degraded state.**

  The specified fan module is not operating at the expected speed.

  Severity
  Warning

  Serviceable

Yes

Automatically notify support
Yes

Alert Category
Cooling Devices (Warning)

SNMP Trap ID
mmTrapFanN

CIM Information
Prefix: CMM **ID:** 0494

User Response
Replace the fan module.

- **000A6006 : Fan module [arg1] is operating in a degraded state.**

  The specified fan module is not operating at the expected speed.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Warning)

  SNMP Trap ID
  mmTrapFanN

  CIM Information
  Prefix: CMM **ID:** 0494

  User Response
  Replace the fan module.

- **000A6007 : Fan module [arg1] is operating in a degraded state.**

  The specified fan module is not operating at the expected speed.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Warning)

  SNMP Trap ID
  mmTrapFanN

  CIM Information
  Prefix: CMM **ID:** 0494

  User Response
  Replace the fan module.

- **000A6008 : Fan module [arg1] is operating in a degraded state.**

  The specified fan module is not operating at the expected speed.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Warning)

  SNMP Trap ID
  mmTrapFanN

  CIM Information
  Prefix: CMM **ID:** 0494

  User Response
  Replace the fan module.
- **000A6009 : Fan module [arg1] is operating in a degraded state.**

  The specified fan module is not operating at the expected speed.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Warning)

  SNMP Trap ID
  mmTrapFanN

  CIM Information
  Prefix: CMM **ID:** 0494

  User Response
  Replace the fan module.
- **000A600A : Fan module [arg1] is operating in a degraded state.**

  The specified fan module is not operating at the expected speed.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Cooling Devices (Warning)

SNMP Trap ID
mmTrapFanN

CIM Information
Prefix: CMM **ID:** 0494

User Response
Replace the fan module.

- **000A9001 : Firmware update of [arg1] controller was not updated.**

  The automatic update of the controller firmware for the specified device was not completed. The Chassis Management Module will automatically restart the update process later.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0702

  User Response
  Information only; no action is required.

- **000A9002 : Firmware update of [arg1] controller was not updated.**

  The automatic update of the controller firmware for the specified device was not completed. The Chassis Management Module will automatically restart the update process later.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0702

  User Response
  Information only; no action is required.

- **000A9003 : Firmware update of [arg1] controller was not updated.**

  The automatic update of the controller firmware for the specified device was not completed. The Chassis Management Module will automatically restart the update process later.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0702

User Response
Information only; no action is required.

- **000A9004 : Firmware update of [arg1] controller was not updated.**

  The automatic update of the controller firmware for the specified device was not completed. The Chassis Management Module will automatically restart the update process later.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0702

  User Response
  Information only; no action is required.

- **000A9005 : Firmware update of [arg1] controller was not updated.**

  The automatic update of the controller firmware for the specified device was not completed. The Chassis Management Module will automatically restart the update process later.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0702

User Response
Information only; no action is required.

- **000A9006 : Firmware update of [arg1] controller was not updated.**

  The automatic update of the controller firmware for the specified device was not completed. The Chassis Management Module will automatically restart the update process later.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0702

  User Response
  Information only; no action is required.

- **000A9007 : Firmware update of [arg1] controller was not updated.**

  The automatic update of the controller firmware for the specified device was not completed. The Chassis Management Module will automatically restart the update process later.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0702

  User Response
  Information only; no action is required.

- **000A9008 : Firmware update of [arg1] controller was not updated.**

  The automatic update of the controller firmware for the specified device was not completed. The Chassis Management Module will automatically restart the update process later.

  Severity
  Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0702

User Response
Information only; no action is required.

- **000A9009 : Firmware update of [arg1] controller was not updated.**

  The automatic update of the controller firmware for the specified device was not completed. The Chassis Management Module will automatically restart the update process later.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0702

  User Response
  Information only; no action is required.

- **000A900A : Firmware update of [arg1] controller was not updated.**

  The automatic update of the controller firmware for the specified device was not completed. The Chassis Management Module will automatically restart the update process later.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0702

User Response
Information only; no action is required.

- **000AA001 : Starting automatic firmware update of [arg1] controller to current version.**

  The controller firmware version of the specified device does not match the current version. The Chassis Management Module will automatically update the controller firmware.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0703

  User Response
  Information only; no action is required.

- **000AA002 : Starting automatic firmware update of [arg1] controller to current version.**

  The controller firmware version of the specified device does not match the current version. The Chassis Management Module will automatically update the controller firmware.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0703

  User Response
  Information only; no action is required.

- **000AA003 : Starting automatic firmware update of [arg1] controller to current version.**

  The controller firmware version of the specified device does not match the current version. The Chassis Management Module will automatically update the controller firmware.

  Severity
  Informational

  Serviceable
  No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0703

User Response
Information only; no action is required.

- **000AA004 : Starting automatic firmware update of [arg1] controller to current version.**

The controller firmware version of the specified device does not match the current version. The Chassis Management Module will automatically update the controller firmware.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0703

User Response
Information only; no action is required.

- **000AA005 : Starting automatic firmware update of [arg1] controller to current version.**

The controller firmware version of the specified device does not match the current version. The Chassis Management Module will automatically update the controller firmware.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0703

User Response
Information only; no action is required.

- **000AA006 : Starting automatic firmware update of [arg1] controller to current version.**

  The controller firmware version of the specified device does not match the current version. The Chassis Management Module will automatically update the controller firmware.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0703

  User Response
  Information only; no action is required.
- **000AA007 : Starting automatic firmware update of [arg1] controller to current version.**

  The controller firmware version of the specified device does not match the current version. The Chassis Management Module will automatically update the controller firmware.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0703

  User Response
  Information only; no action is required.
- **000AA008 : Starting automatic firmware update of [arg1] controller to current version.**

  The controller firmware version of the specified device does not match the current version. The Chassis Management Module will automatically update the controller firmware.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0703

User Response
Information only; no action is required.

- **000AA009 : Starting automatic firmware update of [arg1] controller to current version.**

  The controller firmware version of the specified device does not match the current version. The Chassis Management Module will automatically update the controller firmware.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0703

  User Response
  Information only; no action is required.

- **000AA00A : Starting automatic firmware update of [arg1] controller to current version.**

  The controller firmware version of the specified device does not match the current version. The Chassis Management Module will automatically update the controller firmware.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0703

  User Response
  Information only; no action is required.

- **000AA201 : Starting automatic firmware update of [arg1] controller.**

The controller firmware version for the specified device is unavailable. The Chassis Management Module will automatically update the firmware for this controller.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0704

User Response
Information only; no action is required.

- **000AA202 : Starting automatic firmware update of [arg1] controller.**

The controller firmware version for the specified device is unavailable. The Chassis Management Module will automatically update the firmware for this controller.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0704

User Response
Information only; no action is required.

- **000AA203 : Starting automatic firmware update of [arg1] controller.**

The controller firmware version for the specified device is unavailable. The Chassis Management Module will automatically update the firmware for this controller.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category

Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0704

User Response
Information only; no action is required.

- **000AA204 : Starting automatic firmware update of [arg1] controller.**

  The controller firmware version for the specified device is unavailable. The Chassis Management Module will automatically update the firmware for this controller.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0704

  User Response
  Information only; no action is required.

- **000AA205 : Starting automatic firmware update of [arg1] controller.**

  The controller firmware version for the specified device is unavailable. The Chassis Management Module will automatically update the firmware for this controller.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0704

  User Response
  Information only; no action is required.

- **000AA206 : Starting automatic firmware update of [arg1] controller.**

  The controller firmware version for the specified device is unavailable. The Chassis Management Module will automatically update the firmware for this controller.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0704

User Response
Information only; no action is required.

- **000AA207 : Starting automatic firmware update of [arg1] controller.**

  The controller firmware version for the specified device is unavailable. The Chassis Management Module will automatically update the firmware for this controller.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0704

  User Response
  Information only; no action is required.

- **000AA208 : Starting automatic firmware update of [arg1] controller.**

  The controller firmware version for the specified device is unavailable. The Chassis Management Module will automatically update the firmware for this controller.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0704

User Response
Information only; no action is required.

- **000AA209 : Starting automatic firmware update of [arg1] controller.**

  The controller firmware version for the specified device is unavailable. The Chassis Management Module will automatically update the firmware for this controller.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0704

  User Response
  Information only; no action is required.

- **000AA20A : Starting automatic firmware update of [arg1] controller.**

  The controller firmware version for the specified device is unavailable. The Chassis Management Module will automatically update the firmware for this controller.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0704

  User Response
  Information only; no action is required.

- **000AB001 : Firmware update of [arg1] controller is completed.**

  The automatic update of the controller firmware for the specified device has completed successfully.

  Severity
  Informational

  Serviceable

No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0701

User Response
Information only; no action is required.

- **000AB002 : Firmware update of [arg1] controller is completed.**

  The automatic update of the controller firmware for the specified device has completed successfully.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0701

  User Response
  Information only; no action is required.

- **000AB003 : Firmware update of [arg1] controller is completed.**

  The automatic update of the controller firmware for the specified device has completed successfully.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0701

  User Response
  Information only; no action is required.

- **000AB004 : Firmware update of [arg1] controller is completed.**

  The automatic update of the controller firmware for the specified device has completed successfully.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0701

  User Response
  Information only; no action is required.
- **000AB005 : Firmware update of [arg1] controller is completed.**

  The automatic update of the controller firmware for the specified device has completed successfully.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0701

  User Response
  Information only; no action is required.
- **000AB006 : Firmware update of [arg1] controller is completed.**

  The automatic update of the controller firmware for the specified device has completed successfully.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0701

User Response
Information only; no action is required.

- **000AB007 : Firmware update of [arg1] controller is completed.**

  The automatic update of the controller firmware for the specified device has completed successfully.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0701

  User Response
  Information only; no action is required.

- **000AB008 : Firmware update of [arg1] controller is completed.**

  The automatic update of the controller firmware for the specified device has completed successfully.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0701

  User Response
  Information only; no action is required.

- **000AB009 : Firmware update of [arg1] controller is completed.**

  The automatic update of the controller firmware for the specified device has completed successfully.

  Severity
  Informational

  Serviceable

No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0701

User Response
Information only; no action is required.

- **000AB00A : Firmware update of [arg1] controller is completed.**

  The automatic update of the controller firmware for the specified device has completed successfully.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0701

  User Response
  Information only; no action is required.

- **000FF1BA : The SMTP server at address [arg1] is not reachable.**

  The configured Simple Mail Transfer Protocol (SMTP) server address is not responding and appears to be unreachable.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0274

  User Response

Complete the following steps until the problem is solved:

1. Make sure that the Domain Name System (DNS) server is enabled and configured correctly.
2. Make sure that the SMTP server is operational and that you can communicate with the SMTP server through the Chassis Management Module.
3. Check for network connectivity issues, such as user network cabling and network status.

- **00104201 : Default values restored and Chassis Management Module reset by a long press of the reset button.**

  The specified user has restored the default configuration to the Chassis Management Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0550

  User Response
  Information only; no action is required.

- **00104202 : Default values restored and Chassis Management Module reset by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has restored the default configuration to the Chassis Management Module. If the user did not select the option to preserve the logs, the system and audit logs will be reinitialized.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0551

  User Response
  Information only; no action is required.

- **00104203 : Chassis Management Module reset was initiated by a short press of the reset button.**

  The reset button has been pressed to reset the Chassis Management Module.

  Severity

Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0552

User Response
Information only; no action is required.

- **00104204 : Primary Chassis Management Module reset was initiated by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has reset the primary Chassis Management Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0553

  User Response
  Information only; no action is required.

- **00104205 : Standby Chassis Management Module reset was initiated by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has reset the standby Chassis Management Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0554

User Response
Information only; no action is required.

- **00104206 : Chassis Management Module reset was initiated on the standby CMM by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has reset the primary Chassis Management Module (CMM) from the standby CMM.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0555

  User Response
  Information only; no action is required.

- **00104207 : Chassis Management Module reset was initiated on the primary CMM by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has reset the primary Chassis Management Module (CMM) from the primary CMM.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0556

  User Response
  Information only; no action is required.

- **00104208 : Chassis Management Module [arg1] reset was initiated by user ID [arg2] from [arg3] at IP address [arg4].**

  A service level reset of the CMM was performed by the specified user account.

  Severity
  Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0653

User Response
Information only; no action is required.

- **00104209 : Chassis Management Module [arg1] reset was initiated by user ID [arg2] from [arg3] at IP address [arg4].**

  A service level reset of the CMM was performed by the specified user account.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0653

  User Response
  Information only; no action is required.

- **00104210 : The initial component discovery process is complete. Chassis counter: [arg1] previous: [arg2].**

  The initial chassis component discovery is complete. This does not include node discovery. The current and previous Chassis Management Module (CMM) counters are reported. If the current and previous counters are different, something changed while the CMM was offline. The counter is a unique number that is based on presence and vital product data of the chassis components. It does not include information about the nodes.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0241

User Response
Information only; no action is required.

- **00104211 : Chassis Management Module [arg1] reset by the diagnostics interface.**

  The CMM was reset through the diagnostic interface.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0654

  User Response
  Information only; no action is required.

- **00104212 : Chassis Management Module [arg1] reset by the diagnostics interface.**

  The CMM was reset through the diagnostic interface.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0654

  User Response
  Information only; no action is required.

- **00104221 : Chassis Management Module [arg1] virtual reseat was initiated by user ID [arg2] from [arg3] at IP address [arg4].**

  A service level virtual reseat of the CMM was performed by the specified user account.

  Severity
  Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0742

User Response
Information only; no action is required.

- **00104222 : Chassis Management Module [arg1] virtual reseat was initiated by user ID [arg2] from [arg3] at IP address [arg4].**

  A service level virtual reseat of the CMM was performed by the specified user account.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0742

  User Response
  Information only; no action is required.

- **00120000 : System management (I2C) bus re-initialized.**

  This is a normal corrective action that the Chassis Management Module takes to reset the I2C bus to restore communication with devices. If communication is not restored, another message will be displayed.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0123

User Response
Information only; no action is required.

- **00200000 : Remote login failed for user [arg1] from [arg2] at IP address [arg3].**

  The specified user cannot log in.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0155

  User Response
  Information only; no action is required.

- **00216002 : Node [arg1] system-management processor reset. Persistent events will be regenerated.**

  The system-management processor in the specified node has been reset. Events that are related to the node before the system-management processor was reset will be regenerated if these events are still applicable. However, events that are related to firmware might not be regenerated.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0191

  User Response
  Information only; no action is required.

- **00216005 : NMI reset requested for node [arg1] was not completed.**

  An attempt to restart the specified node with a nonmaskable interrupt (NMI) has failed.

  Severity
  Informational

  Serviceable
  No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0269

User Response
Retry the NMI reset. If the retry fails, consider a hard restart of the system-management processor.

- **00217000 : Chassis Management Module external network physical link broken.**

The Chassis Management Module (CMM) physical link to the external network has been broken. If a standby CMM is installed, a failover will be attempted.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0813

User Response
Complete the following steps until the problem is solved:

1. Make sure that the Ethernet cable is connected (check the connections on both ends of the cable) and that the cable is intact.
2. Make sure that the devices on both ends of the cable are powered on and functioning.

- **00217001 : Chassis Management Module [arg1] external network logical link broken.**

The Chassis Management Module (CMM) logical link to the external network has been broken. If a standby CMM is installed, a failover will be attempted.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information

Prefix: CMM **ID:** 0814

User Response
Make sure that the network is configured correctly and is functioning.

- **00217002 : Physical uplink failover delay settings were changed by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has changed the "Failover delay for physical link loss" setting.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0385

  User Response
  Information only; no action is required.

- **00217003 : Logical uplink failover delay settings were changed by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has changed the "Failover delay for logical link loss" setting.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0386

  User Response
  Information only; no action is required.

- **00217004 : Physical uplink failover was enabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has enabled the failover on the loss of a physical link.

  Severity
  Informational

  Serviceable
  No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0954

User Response
Information only; no action is required.

- **00217005 : Logical uplink failover was enabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has enabled the failover on the loss of a logical link.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0956

  User Response
  Information only; no action is required.

- **00222000 : Standby Chassis Management Module failure on the system management bus. Check devices.**

  The Chassis Management Module (CMM) has detected a failure on the systems-management bus. A failover was initiated, and the primary CMM is now the standby CMM.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0278

  User Response
  Use one of the following procedures:

  - If active problems are reported in the Chassis Management Module log, solve them.
  - If no active bus problems are reported in the log, during scheduled maintenance, swap the physical locations of the primary CMM and the standby CMM. If the problems follow the CMM, replace the CMM. Otherwise, replace the device that is reported in the log.
- **00282001 : Hardware inserted in [arg1].**

  Hardware has been installed in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0100

  User Response
  Information only; no action is required.
- **00282002 : Hardware inserted in [arg1].**

  Hardware has been installed in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0100

  User Response
  Information only; no action is required.
- **00282101 : Discovered device [arg1] in [arg2], CRC: [arg3].**

  Hardware has been discovered successfully in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support

No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0102

User Response
Information only; no action is required.

- **00282102 : Discovered device [arg1] in [arg2], CRC: [arg3].**

  Hardware has been discovered successfully in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0102

  User Response
  Information only; no action is required.

- **00282201 : Failed to discover device [arg1] in [arg2].**

  Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0103

  User Response
  Information only; no action is required.

- **00282202 : Failed to discover device [arg1] in [arg2].**

Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0103

User Response
Information only; no action is required.

- **00284001 : Hardware removed from [arg1].**

Hardware has been removed from the specified bay in the chassis.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0101

User Response
Information only; no action is required.

- **00284002 : Hardware removed from [arg1].**

Hardware has been removed from the specified bay in the chassis.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Inventory change (Informational)

SNMP Trap ID

mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0101

User Response
Information only; no action is required.

- **00285000 : The name of Chassis Management Module in [arg1] was changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The name of the specified Chassis Management Module has been changed to the specified value by the specified user.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0440

  User Response
  Information only; no action is required.

- **04110000 : Detected duplicate IPv6 address [arg1] at MAC address [arg2].**

  The Chassis Management Module has received an ARP request or reply from the specified MAC address. The IPv6 address that was received in the request or reply is already being used by the Chassis Management Module.

  Severity
  Informational

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0574

  User Response
  Make sure that the IPv6 address for all network devices is unique.

- **04110001 : SNMPv3 trap receiver configured for user [arg1] changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

The specified user has changed the Chassis Management Module SNMPv3 trap receiver configuration for the specified user profile.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0393

User Response
Information only; no action is required.

- **04110003 : SNMPv3 context name configured for user [arg1] changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the Chassis Management Module SNMPv3 context name for the specified user profile.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0755

  User Response
  Information only; no action is required.

- **04110004 : SNMPv3 authentication protocol configured for user [arg1] changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the Chassis Management Module SNMPv3 authentication protocol for the specified user profile.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0756

User Response
Information only; no action is required.

- **04110005 : SNMPv3 security level configured for user [arg1] changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the Chassis Management Module SNMPv3 security level for the specified user profile.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0757

  User Response
  Information only; no action is required.

- **04110006 : SNMPv3 access type configured for user [arg1] changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the Chassis Management Module SNMPv3 access type for the specified user profile.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0758

  User Response
  Information only; no action is required.

- **04110007 : SNMPv3 privacy protocol configured for user [arg1] changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the Chassis Management Module SNMPv3 privacy protocol for the specified user profile.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0759

  User Response
  Information only; no action is required.
- **04110008 : Node SNMPv3 trap receiver configured for user [arg1] changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the centrally managed SNMPv3 node account trap receiver configuration.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0846

  User Response
  Information only; no action is required.
- **04110009 : Node SNMPv3 context name configured for user [arg1] changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the centrally managed SNMPv3 node account context name.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support

No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0847

User Response
Information only; no action is required.

- **0411000A : Node SNMPv3 authentication protocol configured for user [arg1] changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the centrally managed SNMPv3 node account authentication protocol.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0848

  User Response
  Information only; no action is required.

- **0411000B : Node SNMPv3 access type configured for user [arg1] changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the centrally managed SNMPv3 node account access type.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0849

  User Response
  Information only; no action is required.

- **0411000C : Node SNMPv3 privacy protocol configured for user [arg1] changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the centrally managed SNMPv3 node account privacy protocol.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0850

  User Response
  Information only; no action is required.
- **04210001 : Node [arg1] system-management processor exited update mode.**

  The system-management processor in the node is not longer in Update mode.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0179

  User Response
  Information only; no action is required.
- **06000201 : Chassis Management Module in CMM bay [arg1] is primary.**

  The Chassis Management Module (CMM) in the specified CMM bay is the primary CMM.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0014

User Response
Information only; no action is required.

- **06000202 : Chassis Management Module in CMM bay [arg1] is primary.**

  The Chassis Management Module (CMM) in the specified CMM bay is the primary CMM.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0014

  User Response
  Information only; no action is required.

- **06000301 : Chassis Management Module in CMM bay [arg1] is standby.**

  The Chassis Management Module (CMM) in the specified CMM bay is now the standby CMM.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0015

  User Response
  Information only; no action is required.

- **06000302 : Chassis Management Module in CMM bay [arg1] is standby.**

  The Chassis Management Module (CMM) in the specified CMM bay is now the standby CMM.

  Severity
  Informational

  Serviceable

No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0015

User Response
Information only; no action is required.

- **0600A001 : Node [arg1] failed initial provisioning.**

The initial node setup has failed.

Severity
Error

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0324

User Response
Perform a service-level reset of the node.

- **0600A002 : Node [arg1] failed initial provisioning.**

The initial node setup has failed.

Severity
Error

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0324

User Response
Perform a service-level reset of the node.

- **0600A003 : Node [arg1] failed initial provisioning.**

  The initial node setup has failed.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Critical)

  SNMP Trap ID
  mmTrapBladeC

  CIM Information
  Prefix: CMM **ID:** 0324

  User Response
  Perform a service-level reset of the node.
- **0600A004 : Node [arg1] failed initial provisioning.**

  The initial node setup has failed.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Critical)

  SNMP Trap ID
  mmTrapBladeC

  CIM Information
  Prefix: CMM **ID:** 0324

  User Response
  Perform a service-level reset of the node.
- **0600A005 : Node [arg1] failed initial provisioning.**

  The initial node setup has failed.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0324

User Response
Perform a service-level reset of the node.

- **0600A006 : Node [arg1] failed initial provisioning.**

  The initial node setup has failed.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Critical)

  SNMP Trap ID
  mmTrapBladeC

  CIM Information
  Prefix: CMM **ID:** 0324

  User Response
  Perform a service-level reset of the node.
- **0600A007 : Node [arg1] failed initial provisioning.**

  The initial node setup has failed.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Critical)

  SNMP Trap ID
  mmTrapBladeC

  CIM Information
  Prefix: CMM **ID:** 0324

  User Response
  Perform a service-level reset of the node.
- **0600A008 : Node [arg1] failed initial provisioning.**

  The initial node setup has failed.

  Severity
  Error

  Serviceable

Yes

Automatically notify support
No

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0324

User Response
Perform a service-level reset of the node.

- **0600A009 : Node [arg1] failed initial provisioning.**

The initial node setup has failed.

Severity
Error

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0324

User Response
Perform a service-level reset of the node.

- **0600A00A : Node [arg1] failed initial provisioning.**

The initial node setup has failed.

Severity
Error

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0324

User Response
Perform a service-level reset of the node.

- **0600A00B : Node [arg1] failed initial provisioning.**

  The initial node setup has failed.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Critical)

  SNMP Trap ID
  mmTrapBladeC

  CIM Information
  Prefix: CMM **ID:** 0324

  User Response
  Perform a service-level reset of the node.
- **0600A00C : Node [arg1] failed initial provisioning.**

  The initial node setup has failed.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Critical)

  SNMP Trap ID
  mmTrapBladeC

  CIM Information
  Prefix: CMM **ID:** 0324

  User Response
  Perform a service-level reset of the node.
- **0600A00D : Node [arg1] failed initial provisioning.**

  The initial node setup has failed.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0324

User Response
Perform a service-level reset of the node.

- **0600A00E : Node [arg1] failed initial provisioning.**

  The initial node setup has failed.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Critical)

  SNMP Trap ID
  mmTrapBladeC

  CIM Information
  Prefix: CMM **ID:** 0324

  User Response
  Perform a service-level reset of the node.

- **0600B001 : The node [arg1] has entered maintenance mode for up to [arg2] minutes.**

  The system-management processor is in maintenance mode. The specified node is in a state in which it might not recover from a reset of the system-management processor or a loss of power.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0249

  User Response
  Do not reset the system-management processor, remove the node, or perform a service-level reset of the node when the node is in maintenance mode.

- **0600B002 : The node [arg1] has entered maintenance mode for up to [arg2] minutes.**

  The system-management processor is in maintenance mode. The specified node is in a state in which it might not recover from a reset of the system-management processor or a loss of power.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0249

User Response
Do not reset the system-management processor, remove the node, or perform a service-level reset of the node when the node is in maintenance mode.

- **0600B003 : The node [arg1] has entered maintenance mode for up to [arg2] minutes.**

The system-management processor is in maintenance mode. The specified node is in a state in which it might not recover from a reset of the system-management processor or a loss of power.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0249

User Response
Do not reset the system-management processor, remove the node, or perform a service-level reset of the node when the node is in maintenance mode.

- **0600B004 : The node [arg1] has entered maintenance mode for up to [arg2] minutes.**

The system-management processor is in maintenance mode. The specified node is in a state in which it might not recover from a reset of the system-management processor or a loss of power.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0249

User Response
Do not reset the system-management processor, remove the node, or perform a service-level reset of the node when the node is in maintenance mode.

- **0600B005 : The node [arg1] has entered maintenance mode for up to [arg2] minutes.**

The system-management processor is in maintenance mode. The specified node is in a state in which it might not recover from a reset of the system-management processor or a loss of power.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0249

User Response
Do not reset the system-management processor, remove the node, or perform a service-level reset of the node when the node is in maintenance mode.

- **0600B006 : The node [arg1] has entered maintenance mode for up to [arg2] minutes.**

The system-management processor is in maintenance mode. The specified node is in a state in which it might not recover from a reset of the system-management processor or a loss of power.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0249

User Response
Do not reset the system-management processor, remove the node, or perform a service-level reset of the node when the node is in maintenance mode.

- **0600B007 : The node [arg1] has entered maintenance mode for up to [arg2] minutes.**

The system-management processor is in maintenance mode. The specified node is in a state in which it might not recover from a reset of the system-management processor or a loss of power.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0249

User Response
Do not reset the system-management processor, remove the node, or perform a service-level reset of the node when the node is in maintenance mode.

- **0600B008 : The node [arg1] has entered maintenance mode for up to [arg2] minutes.**

The system-management processor is in maintenance mode. The specified node is in a state in which it might not recover from a reset of the system-management processor or a loss of power.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0249

User Response
Do not reset the system-management processor, remove the node, or perform a service-level reset of the node when the node is in maintenance mode.

- **0600B009 : The node [arg1] has entered maintenance mode for up to [arg2] minutes.**

The system-management processor is in maintenance mode. The specified node is in a state in which it might not recover from a reset of the system-management processor or a loss of power.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0249

User Response
Do not reset the system-management processor, remove the node, or perform a service-level reset of the node when the node is in maintenance mode.

- **0600B00A : The node [arg1] has entered maintenance mode for up to [arg2] minutes.**

The system-management processor is in maintenance mode. The specified node is in a state in which it might not recover from a reset of the system-management processor or a loss of power.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0249

User Response
Do not reset the system-management processor, remove the node, or perform a service-level reset of the node when the node is in maintenance mode.

- **0600B00B : The node [arg1] has entered maintenance mode for up to [arg2] minutes.**

The system-management processor is in maintenance mode. The specified node is in a state in which it might not recover from a reset of the system-management processor or a loss of power.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0249

User Response

Do not reset the system-management processor, remove the node, or perform a service-level reset of the node when the node is in maintenance mode.

- **0600B00C : The node [arg1] has entered maintenance mode for up to [arg2] minutes.**

  The system-management processor is in maintenance mode. The specified node is in a state in which it might not recover from a reset of the system-management processor or a loss of power.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0249

  User Response
  Do not reset the system-management processor, remove the node, or perform a service-level reset of the node when the node is in maintenance mode.

- **0600B00D : The node [arg1] has entered maintenance mode for up to [arg2] minutes.**

  The system-management processor is in maintenance mode. The specified node is in a state in which it might not recover from a reset of the system-management processor or a loss of power.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0249

  User Response
  Do not reset the system-management processor, remove the node, or perform a service-level reset of the node when the node is in maintenance mode.

- **0600B00E : The node [arg1] has entered maintenance mode for up to [arg2] minutes.**

  The system-management processor is in maintenance mode. The specified node is in a state in which it might not recover from a reset of the system-management processor or a loss of power.

  Severity
  Informational

  Serviceable

No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0249

User Response
Do not reset the system-management processor, remove the node, or perform a service-level reset of the node when the node is in maintenance mode.

- **0600B011 : The node [arg1] is not in maintenance mode.**

The node is not in maintenance mode.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0250

User Response
Information only; no action is required.

- **0600B012 : The node [arg1] is not in maintenance mode.**

The node is not in maintenance mode.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0250

User Response

Information only; no action is required.

- **0600B013 : The node [arg1] is not in maintenance mode.**

  The node is not in maintenance mode.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0250

  User Response
  Information only; no action is required.

- **0600B014 : The node [arg1] is not in maintenance mode.**

  The node is not in maintenance mode.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0250

  User Response
  Information only; no action is required.

- **0600B015 : The node [arg1] is not in maintenance mode.**

  The node is not in maintenance mode.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0250

User Response
Information only; no action is required.

- **0600B016 : The node [arg1] is not in maintenance mode.**

  The node is not in maintenance mode.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0250

  User Response
  Information only; no action is required.

- **0600B017 : The node [arg1] is not in maintenance mode.**

  The node is not in maintenance mode.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0250

  User Response
  Information only; no action is required.

- **0600B018 : The node [arg1] is not in maintenance mode.**

  The node is not in maintenance mode.

  Severity
  Informational

  Serviceable

No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0250

User Response
Information only; no action is required.

- **0600B019 : The node [arg1] is not in maintenance mode.**

The node is not in maintenance mode.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0250

User Response
Information only; no action is required.

- **0600B01A : The node [arg1] is not in maintenance mode.**

The node is not in maintenance mode.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0250

User Response
Information only; no action is required.

- **0600B01B : The node [arg1] is not in maintenance mode.**

  The node is not in maintenance mode.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0250

  User Response
  Information only; no action is required.
- **0600B01C : The node [arg1] is not in maintenance mode.**

  The node is not in maintenance mode.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0250

  User Response
  Information only; no action is required.
- **0600B01D : The node [arg1] is not in maintenance mode.**

  The node is not in maintenance mode.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0250

User Response
Information only; no action is required.

- **0600B01E : The node [arg1] is not in maintenance mode.**

The node is not in maintenance mode.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0250

User Response
Information only; no action is required.

- **0600C001 : The node [arg1] is saving cached data to disk.**

The specified node is saving its volatile cache and system data to disk.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0255

User Response
Do not reset the system-management processor, remove the node from the Flex System chassis, or perform a service reset of the node when cache is being flushed to disk.

- **0600C002 : The node [arg1] is saving cached data to disk.**

The specified node is saving its volatile cache and system data to disk.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0255

User Response
Do not reset the system-management processor, remove the node from the Flex System chassis, or perform a service reset of the node when cache is being flushed to disk.

- **0600C003 : The node [arg1] is saving cached data to disk.**

The specified node is saving its volatile cache and system data to disk.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0255

User Response
Do not reset the system-management processor, remove the node from the Flex System chassis, or perform a service reset of the node when cache is being flushed to disk.

- **0600C004 : The node [arg1] is saving cached data to disk.**

The specified node is saving its volatile cache and system data to disk.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0255

User Response
Do not reset the system-management processor, remove the node from the Flex System chassis, or perform a service reset of the node when cache is being flushed to disk.

- **0600C005 : The node [arg1] is saving cached data to disk.**

  The specified node is saving its volatile cache and system data to disk.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0255

  User Response
  Do not reset the system-management processor, remove the node from the Flex System chassis, or perform a service reset of the node when cache is being flushed to disk.

- **0600C006 : The node [arg1] is saving cached data to disk.**

  The specified node is saving its volatile cache and system data to disk.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0255

  User Response
  Do not reset the system-management processor, remove the node from the Flex System chassis, or perform a service reset of the node when cache is being flushed to disk.

- **0600C007 : The node [arg1] is saving cached data to disk.**

  The specified node is saving its volatile cache and system data to disk.

  Severity
  Informational

  Serviceable
  No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0255

User Response
Do not reset the system-management processor, remove the node from the Flex System chassis, or perform a service reset of the node when cache is being flushed to disk.

- **0600C008 : The node [arg1] is saving cached data to disk.**

The specified node is saving its volatile cache and system data to disk.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0255

User Response
Do not reset the system-management processor, remove the node from the Flex System chassis, or perform a service reset of the node when cache is being flushed to disk.

- **0600C009 : The node [arg1] is saving cached data to disk.**

The specified node is saving its volatile cache and system data to disk.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0255

User Response

Do not reset the system-management processor, remove the node from the Flex System chassis, or perform a service reset of the node when cache is being flushed to disk.

- **0600C00A : The node [arg1] is saving cached data to disk.**

  The specified node is saving its volatile cache and system data to disk.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0255

  User Response
  Do not reset the system-management processor, remove the node from the Flex System chassis, or perform a service reset of the node when cache is being flushed to disk.

- **0600C00B : The node [arg1] is saving cached data to disk.**

  The specified node is saving its volatile cache and system data to disk.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0255

  User Response
  Do not reset the system-management processor, remove the node from the Flex System chassis, or perform a service reset of the node when cache is being flushed to disk.

- **0600C00C : The node [arg1] is saving cached data to disk.**

  The specified node is saving its volatile cache and system data to disk.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support

No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0255

User Response
Do not reset the system-management processor, remove the node from the Flex System chassis, or perform a service reset of the node when cache is being flushed to disk.

- **0600C00D : The node [arg1] is saving cached data to disk.**

The specified node is saving its volatile cache and system data to disk.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0255

User Response
Do not reset the system-management processor, remove the node from the Flex System chassis, or perform a service reset of the node when cache is being flushed to disk.

- **0600C00E : The node [arg1] is saving cached data to disk.**

The specified node is saving its volatile cache and system data to disk.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0255

User Response
Do not reset the system-management processor, remove the node from the Flex System chassis, or perform a service reset of the node when cache is being flushed to disk.

- **0600C011 : The node [arg1] has exited saving cached data to disk mode.**

  The node has exited saving cached data to disk mode.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0256

  User Response
  Information only; no action is required.
- **0600C012 : The node [arg1] has exited saving cached data to disk mode.**

  The node has exited saving cached data to disk mode.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0256

  User Response
  Information only; no action is required.
- **0600C013 : The node [arg1] has exited saving cached data to disk mode.**

  The node has exited saving cached data to disk mode.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0256

User Response
Information only; no action is required.

- **0600C014 : The node [arg1] has exited saving cached data to disk mode.**

  The node has exited saving cached data to disk mode.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0256

  User Response
  Information only; no action is required.

- **0600C015 : The node [arg1] has exited saving cached data to disk mode.**

  The node has exited saving cached data to disk mode.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0256

  User Response
  Information only; no action is required.

- **0600C016 : The node [arg1] has exited saving cached data to disk mode.**

  The node has exited saving cached data to disk mode.

  Severity
  Informational

  Serviceable

No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0256

User Response
Information only; no action is required.

- **0600C017 : The node [arg1] has exited saving cached data to disk mode.**

  The node has exited saving cached data to disk mode.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0256

  User Response
  Information only; no action is required.

- **0600C018 : The node [arg1] has exited saving cached data to disk mode.**

  The node has exited saving cached data to disk mode.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0256

  User Response
  Information only; no action is required.

- **0600C019 : The node [arg1] has exited saving cached data to disk mode.**

  The node has exited saving cached data to disk mode.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0256

  User Response
  Information only; no action is required.
- **0600C01A : The node [arg1] has exited saving cached data to disk mode.**

  The node has exited saving cached data to disk mode.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0256

  User Response
  Information only; no action is required.
- **0600C01B : The node [arg1] has exited saving cached data to disk mode.**

  The node has exited saving cached data to disk mode.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0256

User Response
Information only; no action is required.

- **0600C01C : The node [arg1] has exited saving cached data to disk mode.**

  The node has exited saving cached data to disk mode.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0256

  User Response
  Information only; no action is required.

- **0600C01D : The node [arg1] has exited saving cached data to disk mode.**

  The node has exited saving cached data to disk mode.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0256

  User Response
  Information only; no action is required.

- **0600C01E : The node [arg1] has exited saving cached data to disk mode.**

  The node has exited saving cached data to disk mode.

  Severity
  Informational

  Serviceable

No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0256

User Response
Information only; no action is required.

- **06100000 : Chassis Machine Type Model has not been programmed in the midplane EEPROM. Previous MTM is [arg1].**

  The chassis Machine Type Model has not been programmed in the midplane EEPROM.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0663

  User Response
  Use the correct service procedure to update the midplane EEPROM.

- **06200000 : Chassis Serial Number has not been programmed in the midplane EEPROM. Previous SN is [arg1].**

  The chassis Serial Number has not been programmed in the midplane EEPROM.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0664

User Response
Use the correct service procedure to update the midplane EEPROM.

- **06300000 : Chassis UUID has not been programmed in the midplane EEPROM. Previous UUID is [arg1].**

  The chassis UUID has not been programmed in the midplane EEPROM.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0665

  User Response
  Use the correct service procedure to update the midplane EEPROM.

- **06A2E001 : Chassis temperature device is unavailable.**

  The chassis temperature is unavailable or unreadable from the rear LED card. The cooling capacity of the chassis has been set to the maximum, and the fan modules are running at full speed.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0158

  User Response
  Check the Chassis Management Module event log for communication failures for multiple components, such as I/O modules, fan modules, and power supplies. If there are communication failures for multiple components, restart the Chassis Management Module. If there are no other communication failures, replace the rear LED card.

- **0800A401 : Acoustic mode policy was changed by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has changed the acoustic mode policy.

  Severity
  Informational

  Serviceable

No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0923

User Response
Information only; no action is required.

- **0800A402 : NEBS mode policy changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has enabled or disabled the NEBS mode policy.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0838

  User Response
  Information only; no action is required.

- **0800A403 : Acoustic mode policy was enabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has disabled the acoustic mode policy.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0907

  User Response
  Information only; no action is required.

- **0800A404 : Acoustic mode policy was disabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has disabled the acoustic mode policy.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0908

  User Response
  Information only; no action is required.
- **0800A405 : Secure CIM-XML was disabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has disabled the secure CIM-XML port.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0929

  User Response
  Information only; no action is required.
- **0800A406 : SSL server was disabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has disabled the Secure Sockets Layer (SSL) server.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0931

User Response
Information only; no action is required.

- **0800A407 : SSL client was disabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has disabled the Secure Sockets Layer (SSL) client.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0933

  User Response
  Information only; no action is required.

- **0800B401 : Power policy was changed to Power Module Redundancy by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has changed the power management policy to Power Module Redundancy.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0938

  User Response
  Information only; no action is required.

- **0800B402 : Power policy was changed to Power Module Redundancy with Blade Throttling Allowed by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has changed the power management policy to Power Module Redundancy with Blade Throttling Allowed.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0939

User Response
Information only; no action is required.

- **0800B403 : Power policy was changed to Basic Power Management by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has changed the power management policy to Basic Power Management.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0940

  User Response
  Information only; no action is required.

- **0800B404 : Power policy was changed to Power Source Redundancy by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has changed the power management policy to Power Source Redundancy.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0941

User Response
Information only; no action is required.

- **0800B405 : Power policy was changed to Power Source Redundancy with Blade Throttling Allowed by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has changed the power management policy to Power Source Redundancy with Blade Throttling Allowed.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0942

  User Response
  Information only; no action is required.

- **0800B406 : Physical uplink failover was disabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has disabled the failover on the loss of a physical link.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0955

  User Response
  Information only; no action is required.

- **0800B407 : Logical uplink failover was disabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has disabled the failover on the loss of a logical link.

  Severity
  Informational

  Serviceable

No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0957

User Response
Information only; no action is required.

- **0800C401 : Data sampling interval changed to [arg1] minutes by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the power trend sampling interval.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0163

  User Response
  Information only; no action is required.

- **0800D401 : Power capping level changed to [arg1] on node [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the power capping level for a node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0164

User Response
Information only; no action is required.

- **0800E401 : Aggregate power capping level changed to [arg1] on node [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the aggregate power capping level for a node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0165

  User Response
  Information only; no action is required.

- **0800F401 : Power control [arg1] changed to [arg2] on node [arg3] by user ID [arg4] from [arg5] at IP address [arg6].**

  The specified user has enabled or disabled the power capping control of a node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0166

  User Response
  Information only; no action is required.

- **08028001 : Power supply [arg1] is off. DC fault.**

  A dc fault has occurred in the specified power supply, and the power supply will shut down. Events related to loss of power redundancy might also be reported in the Chassis Management Module event log.

  Severity
  Error

  Serviceable
  Yes

Automatically notify support
Yes

Alert Category
Power Modules (Critical)

SNMP Trap ID
mmTrapPsC

CIM Information
Prefix: CMM **ID:** 0037

User Response
Replace the power supply.

- **08028002 : Power supply [arg1] is off. DC fault.**

  A dc fault has occurred in the specified power supply, and the power supply will shut down. Events related to loss of power redundancy might also be reported in the Chassis Management Module event log.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Critical)

  SNMP Trap ID
  mmTrapPsC

  CIM Information
  Prefix: CMM **ID:** 0037

  User Response
  Replace the power supply.

- **08028003 : Power supply [arg1] is off. DC fault.**

  A dc fault has occurred in the specified power supply, and the power supply will shut down. Events related to loss of power redundancy might also be reported in the Chassis Management Module event log.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Critical)

  SNMP Trap ID
  mmTrapPsC

  CIM Information
  Prefix: CMM **ID:** 0037

  User Response
  Replace the power supply.

- **08028004 : Power supply [arg1] is off. DC fault.**

  A dc fault has occurred in the specified power supply, and the power supply will shut down. Events related to loss of power redundancy might also be reported in the Chassis Management Module event log.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Critical)

  SNMP Trap ID
  mmTrapPsC

  CIM Information
  Prefix: CMM **ID:** 0037

  User Response
  Replace the power supply.
- **08028005 : Power supply [arg1] is off. DC fault.**

  A dc fault has occurred in the specified power supply, and the power supply will shut down. Events related to loss of power redundancy might also be reported in the Chassis Management Module event log.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Critical)

  SNMP Trap ID
  mmTrapPsC

  CIM Information
  Prefix: CMM **ID:** 0037

  User Response
  Replace the power supply.
- **08028006 : Power supply [arg1] is off. DC fault.**

  A dc fault has occurred in the specified power supply, and the power supply will shut down. Events related to loss of power redundancy might also be reported in the Chassis Management Module event log.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

Alert Category
Power Modules (Critical)

SNMP Trap ID
mmTrapPsC

CIM Information
Prefix: CMM **ID:** 0037

User Response
Replace the power supply.

- **08028481 : Power supply [arg1] is off. Input fault.**

  The specified power supply does not have input power.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Power Modules (Warning)

  SNMP Trap ID
  mmTrapPowerN

  CIM Information
  Prefix: CMM **ID:** 0043

  User Response
  Restore input to the power supply.

- **08028482 : Power supply [arg1] is off. Input fault.**

  The specified power supply does not have input power.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Power Modules (Warning)

  SNMP Trap ID
  mmTrapPowerN

  CIM Information
  Prefix: CMM **ID:** 0043

  User Response
  Restore input to the power supply.

- **08028483 : Power supply [arg1] is off. Input fault.**

  The specified power supply does not have input power.

  Severity

Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Power Modules (Warning)

SNMP Trap ID
mmTrapPowerN

CIM Information
Prefix: CMM **ID:** 0043

User Response
Restore input to the power supply.

- **08028484 : Power supply [arg1] is off. Input fault.**

  The specified power supply does not have input power.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Power Modules (Warning)

  SNMP Trap ID
  mmTrapPowerN

  CIM Information
  Prefix: CMM **ID:** 0043

  User Response
  Restore input to the power supply.

- **08028485 : Power supply [arg1] is off. Input fault.**

  The specified power supply does not have input power.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Power Modules (Warning)

  SNMP Trap ID
  mmTrapPowerN

  CIM Information
  Prefix: CMM **ID:** 0043

User Response
Restore input to the power supply.

- **08028486 : Power supply [arg1] is off. Input fault.**

  The specified power supply does not have input power.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Power Modules (Warning)

  SNMP Trap ID
  mmTrapPowerN

  CIM Information
  Prefix: CMM **ID:** 0043

  User Response
  Restore input to the power supply.

- **08080001 : Insufficient chassis power supplies to support redundancy.**

  The number of power supplies within a power domain is not sufficient to support power supply redundancy in the selected power policy. This can occur because not enough power supplies are installed or because a power supply has failed.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Power Modules (Warning)

  SNMP Trap ID
  mmTrapPowerN

  CIM Information
  Prefix: CMM **ID:** 0243

  User Response
  Use one of the following procedures:
  - If redundancy is required, install additional power supplies.
  - If a power supply has failed, replace that power supply.

- **08200001 : Power supply [arg1] communication is offline.**

  The power supply has failed to communicate with the systems-management software. It might or might not be providing power.

  Severity
  Error

  Serviceable

Yes

Automatically notify support
Yes

Alert Category
Power Modules (Critical)

SNMP Trap ID
mmTrapPsC

CIM Information
Prefix: CMM **ID:** 0236

User Response
Replace the power supply.

- **08200002 : Power supply [arg1] communication is offline.**

  The power supply has failed to communicate with the systems-management software. It might or might not be providing power.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Critical)

  SNMP Trap ID
  mmTrapPsC

  CIM Information
  Prefix: CMM **ID:** 0236

  User Response
  Replace the power supply.

- **08200003 : Power supply [arg1] communication is offline.**

  The power supply has failed to communicate with the systems-management software. It might or might not be providing power.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Critical)

  SNMP Trap ID
  mmTrapPsC

  CIM Information
  Prefix: CMM **ID:** 0236

User Response
Replace the power supply.

- **08200004 : Power supply [arg1] communication is offline.**

  The power supply has failed to communicate with the systems-management software. It might or might not be providing power.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Critical)

  SNMP Trap ID
  mmTrapPsC

  CIM Information
  Prefix: CMM **ID:** 0236

  User Response
  Replace the power supply.

- **08200005 : Power supply [arg1] communication is offline.**

  The power supply has failed to communicate with the systems-management software. It might or might not be providing power.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Critical)

  SNMP Trap ID
  mmTrapPsC

  CIM Information
  Prefix: CMM **ID:** 0236

  User Response
  Replace the power supply.

- **08200006 : Power supply [arg1] communication is offline.**

  The power supply has failed to communicate with the systems-management software. It might or might not be providing power.

  Severity
  Error

  Serviceable
  Yes

Automatically notify support
Yes

Alert Category
Power Modules (Critical)

SNMP Trap ID
mmTrapPsC

CIM Information
Prefix: CMM **ID:** 0236

User Response
Replace the power supply.

- **08216001 : Hardware inserted in [arg1].**

Hardware has been installed in the specified bay in the chassis.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0100

User Response
Information only; no action is required.

- **08216002 : Hardware inserted in [arg1].**

Hardware has been installed in the specified bay in the chassis.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0100

User Response
Information only; no action is required.

- **08216003 : Hardware inserted in [arg1].**

Hardware has been installed in the specified bay in the chassis.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0100

User Response
Information only; no action is required.

- **08216004 : Hardware inserted in [arg1].**

Hardware has been installed in the specified bay in the chassis.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0100

User Response
Information only; no action is required.

- **08216005 : Hardware inserted in [arg1].**

Hardware has been installed in the specified bay in the chassis.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0100

User Response
Information only; no action is required.

- **08216006 : Hardware inserted in [arg1].**

  Hardware has been installed in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0100

  User Response
  Information only; no action is required.

- **08216101 : Discovered device [arg1] in [arg2], CRC: [arg3].**

  Hardware has been discovered successfully in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0102

  User Response
  Information only; no action is required.

- **08216102 : Discovered device [arg1] in [arg2], CRC: [arg3].**

  Hardware has been discovered successfully in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support

No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0102

User Response
Information only; no action is required.

- **08216103 : Discovered device [arg1] in [arg2], CRC: [arg3].**

  Hardware has been discovered successfully in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0102

  User Response
  Information only; no action is required.

- **08216104 : Discovered device [arg1] in [arg2], CRC: [arg3].**

  Hardware has been discovered successfully in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0102

  User Response
  Information only; no action is required.

- **08216105 : Discovered device [arg1] in [arg2], CRC: [arg3].**

  Hardware has been discovered successfully in the specified bay in the chassis.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0102

User Response
Information only; no action is required.

- **08216106 : Discovered device [arg1] in [arg2], CRC: [arg3].**

  Hardware has been discovered successfully in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0102

  User Response
  Information only; no action is required.

- **08216201 : Failed to discover device [arg1] in [arg2].**

  Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0103

User Response
Information only; no action is required.

- **08216202 : Failed to discover device [arg1] in [arg2].**

  Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0103

  User Response
  Information only; no action is required.

- **08216203 : Failed to discover device [arg1] in [arg2].**

  Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0103

  User Response
  Information only; no action is required.

- **08216204 : Failed to discover device [arg1] in [arg2].**

  Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

  Severity
  Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0103

User Response
Information only; no action is required.

- **08216205 : Failed to discover device [arg1] in [arg2].**

  Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0103

  User Response
  Information only; no action is required.

- **08216206 : Failed to discover device [arg1] in [arg2].**

  Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0103

User Response
Information only; no action is required.

- **08216301 : Mismatched power supplies in the chassis: [arg1]. The configuration is not supported.**

  The power supplies in the chassis have mismatched power capacities. All power supplies should have identical power capacities.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0651

  User Response
  Replace the mismatched power supplies in the chassis.

- **08216311 : Mismatched power supply capacities due to input AC voltage level: [arg1].**

  The power supplies in the chassis have mismatched power capacities due to different AC input level. Some power supplies detect the input voltage level to be in the low range (200-218) and others detect the input voltage level to be in high range (220-240).

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0635

  User Response
  Check the AC input voltage levels. The system will operate normally under the current condition. However, the power budget will be based off of the lowest input range capacity. Refer to Retain Tip H21853.

- **08216321 : Chassis power supplies are of mismatched input type: [arg1].**

  The power supplies in the chassis are of mismatched input type. Some accept AC input and some accept DC input.

  Severity
  Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0330

User Response
Check the input feed of the power supplies. It is informational only.

- **0821C001 : Power supply [arg1] has exceeded the warning temperature.**

The temperature of the specified power supply has exceeded the warning threshold. The system is currently operating within the allowed temperature range. However, an additional rise in temperature might result in the shutdown of devices in the chassis.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Power Modules (Warning)

SNMP Trap ID
mmTrapPowerN

CIM Information
Prefix: CMM **ID:** 0024

User Response
Complete the following steps until the problem is solved:

1. Check the Chassis Management Module event log for any events related to the fan modules, and solve those events.
2. Check the ambient room temperature to ensure that the room is not too hot.
3. Check for any blockage on or near the ventilation holes on the chassis. Remove any blockages that you find.
4. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that nothing is covering the bays. Empty bays can cause a reduction in airflow to the devices in the chassis.
5. Check the ambient chassis temperature. Make sure that enough fan modules are installed to sufficiently cool the devices in the chassis. See the chassis documentation to determine how many fan modules should be installed.
6. Check the status of the specified power supply. If the internal fan has failed, replace the power supply.

- **0821C002 : Power supply [arg1] has exceeded the warning temperature.**

The temperature of the specified power supply has exceeded the warning threshold. The system is currently operating within the allowed temperature range. However, an additional rise in temperature might result in the shutdown of devices in the chassis.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Power Modules (Warning)

SNMP Trap ID
mmTrapPowerN

CIM Information
Prefix: CMM **ID:** 0024

User Response
Complete the following steps until the problem is solved:

1. Check the Chassis Management Module event log for any events related to the fan modules, and solve those events.
2. Check the ambient room temperature to ensure that the room is not too hot.
3. Check for any blockage on or near the ventilation holes on the chassis. Remove any blockages that you find.
4. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that nothing is covering the bays. Empty bays can cause a reduction in airflow to the devices in the chassis.
5. Check the ambient chassis temperature. Make sure that enough fan modules are installed to sufficiently cool the devices in the chassis. See the chassis documentation to determine how many fan modules should be installed.
6. Check the status of the specified power supply. If the internal fan has failed, replace the power supply.

- **0821C003 : Power supply [arg1] has exceeded the warning temperature.**

The temperature of the specified power supply has exceeded the warning threshold. The system is currently operating within the allowed temperature range. However, an additional rise in temperature might result in the shutdown of devices in the chassis.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Power Modules (Warning)

SNMP Trap ID
mmTrapPowerN

CIM Information

Prefix: CMM **ID:** 0024

User Response

Complete the following steps until the problem is solved:

1. Check the Chassis Management Module event log for any events related to the fan modules, and solve those events.
2. Check the ambient room temperature to ensure that the room is not too hot.
3. Check for any blockage on or near the ventilation holes on the chassis. Remove any blockages that you find.
4. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that nothing is covering the bays. Empty bays can cause a reduction in airflow to the devices in the chassis.
5. Check the ambient chassis temperature. Make sure that enough fan modules are installed to sufficiently cool the devices in the chassis. See the chassis documentation to determine how many fan modules should be installed.
6. Check the status of the specified power supply. If the internal fan has failed, replace the power supply.

- **0821C004 : Power supply [arg1] has exceeded the warning temperature.**

The temperature of the specified power supply has exceeded the warning threshold. The system is currently operating within the allowed temperature range. However, an additional rise in temperature might result in the shutdown of devices in the chassis.

Severity

Warning

Serviceable

Yes

Automatically notify support

No

Alert Category

Power Modules (Warning)

SNMP Trap ID

mmTrapPowerN

CIM Information

Prefix: CMM **ID:** 0024

User Response

Complete the following steps until the problem is solved:

1. Check the Chassis Management Module event log for any events related to the fan modules, and solve those events.
2. Check the ambient room temperature to ensure that the room is not too hot.
3. Check for any blockage on or near the ventilation holes on the chassis. Remove any blockages that you find.
4. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that nothing is covering the bays. Empty bays can cause a reduction in airflow to the devices in the chassis.
5. Check the ambient chassis temperature. Make sure that enough fan modules are installed to sufficiently cool the devices in the chassis. See the chassis documentation to determine how many fan modules should be installed.

6. Check the status of the specified power supply. If the internal fan has failed, replace the power supply.

- **0821C005 : Power supply [arg1] has exceeded the warning temperature.**

  The temperature of the specified power supply has exceeded the warning threshold. The system is currently operating within the allowed temperature range. However, an additional rise in temperature might result in the shutdown of devices in the chassis.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Power Modules (Warning)

  SNMP Trap ID
  mmTrapPowerN

  CIM Information
  Prefix: CMM **ID:** 0024

  User Response
  Complete the following steps until the problem is solved:

  1. Check the Chassis Management Module event log for any events related to the fan modules, and solve those events.
  2. Check the ambient room temperature to ensure that the room is not too hot.
  3. Check for any blockage on or near the ventilation holes on the chassis. Remove any blockages that you find.
  4. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that nothing is covering the bays. Empty bays can cause a reduction in airflow to the devices in the chassis.
  5. Check the ambient chassis temperature. Make sure that enough fan modules are installed to sufficiently cool the devices in the chassis. See the chassis documentation to determine how many fan modules should be installed.
  6. Check the status of the specified power supply. If the internal fan has failed, replace the power supply.

- **0821C006 : Power supply [arg1] has exceeded the warning temperature.**

  The temperature of the specified power supply has exceeded the warning threshold. The system is currently operating within the allowed temperature range. However, an additional rise in temperature might result in the shutdown of devices in the chassis.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Power Modules (Warning)

SNMP Trap ID
mmTrapPowerN

CIM Information
Prefix: CMM **ID:** 0024

User Response
Complete the following steps until the problem is solved:

1. Check the Chassis Management Module event log for any events related to the fan modules, and solve those events.
2. Check the ambient room temperature to ensure that the room is not too hot.
3. Check for any blockage on or near the ventilation holes on the chassis. Remove any blockages that you find.
4. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that nothing is covering the bays. Empty bays can cause a reduction in airflow to the devices in the chassis.
5. Check the ambient chassis temperature. Make sure that enough fan modules are installed to sufficiently cool the devices in the chassis. See the chassis documentation to determine how many fan modules should be installed.
6. Check the status of the specified power supply. If the internal fan has failed, replace the power supply.

- **0821C081 : Power supply [arg1] temperature fault.**

A temperature fault has occurred in the specified power supply. A power supply shuts down within 60 seconds of a temperature fault.

Severity
Error

Serviceable
Yes

Automatically notify support
No

Alert Category
Power Modules (Critical)

SNMP Trap ID
mmTrapPsC

CIM Information
Prefix: CMM **ID:** 0023

User Response
Complete the following steps until the problem is solved:

1. Check the Chassis Management Module event log for any events related to the fan modules, and solve those events.
2. Check the ambient room temperature to ensure that the room is not too hot.
3. Check for any blockage on or near the ventilation holes on the chassis. Remove any blockages that you find.
4. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that nothing is covering the bays. Empty bays can cause a reduction in airflow to the devices in the chassis.

5. Check the ambient chassis temperature. Make sure that enough fan modules are installed to sufficiently cool the devices in the chassis. See the chassis documentation to determine how many fan modules should be installed.
6. Check the status of the specified power supply. If the internal fan has failed, replace the power supply.

- **0821C082 : Power supply [arg1] temperature fault.**

  A temperature fault has occurred in the specified power supply. A power supply shuts down within 60 seconds of a temperature fault.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Power Modules (Critical)

  SNMP Trap ID
  mmTrapPsC

  CIM Information
  Prefix: CMM **ID:** 0023

  User Response
  Complete the following steps until the problem is solved:

  1. Check the Chassis Management Module event log for any events related to the fan modules, and solve those events.
  2. Check the ambient room temperature to ensure that the room is not too hot.
  3. Check for any blockage on or near the ventilation holes on the chassis. Remove any blockages that you find.
  4. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that nothing is covering the bays. Empty bays can cause a reduction in airflow to the devices in the chassis.
  5. Check the ambient chassis temperature. Make sure that enough fan modules are installed to sufficiently cool the devices in the chassis. See the chassis documentation to determine how many fan modules should be installed.
  6. Check the status of the specified power supply. If the internal fan has failed, replace the power supply.

- **0821C083 : Power supply [arg1] temperature fault.**

  A temperature fault has occurred in the specified power supply. A power supply shuts down within 60 seconds of a temperature fault.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category

Power Modules (Critical)

SNMP Trap ID
mmTrapPsC

CIM Information
Prefix: CMM **ID:** 0023

User Response
Complete the following steps until the problem is solved:

1. Check the Chassis Management Module event log for any events related to the fan modules, and solve those events.
2. Check the ambient room temperature to ensure that the room is not too hot.
3. Check for any blockage on or near the ventilation holes on the chassis. Remove any blockages that you find.
4. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that nothing is covering the bays. Empty bays can cause a reduction in airflow to the devices in the chassis.
5. Check the ambient chassis temperature. Make sure that enough fan modules are installed to sufficiently cool the devices in the chassis. See the chassis documentation to determine how many fan modules should be installed.
6. Check the status of the specified power supply. If the internal fan has failed, replace the power supply.

- **0821C084 : Power supply [arg1] temperature fault.**

A temperature fault has occurred in the specified power supply. A power supply shuts down within 60 seconds of a temperature fault.

Severity
Error

Serviceable
Yes

Automatically notify support
No

Alert Category
Power Modules (Critical)

SNMP Trap ID
mmTrapPsC

CIM Information
Prefix: CMM **ID:** 0023

User Response
Complete the following steps until the problem is solved:

1. Check the Chassis Management Module event log for any events related to the fan modules, and solve those events.
2. Check the ambient room temperature to ensure that the room is not too hot.
3. Check for any blockage on or near the ventilation holes on the chassis. Remove any blockages that you find.
4. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that nothing is covering the bays. Empty bays can cause a reduction in airflow to the devices in the chassis.

5. Check the ambient chassis temperature. Make sure that enough fan modules are installed to sufficiently cool the devices in the chassis. See the chassis documentation to determine how many fan modules should be installed.
6. Check the status of the specified power supply. If the internal fan has failed, replace the power supply.

- **0821C085 : Power supply [arg1] temperature fault.**

  A temperature fault has occurred in the specified power supply. A power supply shuts down within 60 seconds of a temperature fault.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Power Modules (Critical)

  SNMP Trap ID
  mmTrapPsC

  CIM Information
  Prefix: CMM **ID:** 0023

  User Response
  Complete the following steps until the problem is solved:

  1. Check the Chassis Management Module event log for any events related to the fan modules, and solve those events.
  2. Check the ambient room temperature to ensure that the room is not too hot.
  3. Check for any blockage on or near the ventilation holes on the chassis. Remove any blockages that you find.
  4. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that nothing is covering the bays. Empty bays can cause a reduction in airflow to the devices in the chassis.
  5. Check the ambient chassis temperature. Make sure that enough fan modules are installed to sufficiently cool the devices in the chassis. See the chassis documentation to determine how many fan modules should be installed.
  6. Check the status of the specified power supply. If the internal fan has failed, replace the power supply.

- **0821C086 : Power supply [arg1] temperature fault.**

  A temperature fault has occurred in the specified power supply. A power supply shuts down within 60 seconds of a temperature fault.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category

Power Modules (Critical)

SNMP Trap ID
mmTrapPsC

CIM Information
Prefix: CMM **ID:** 0023

User Response
Complete the following steps until the problem is solved:

1. Check the Chassis Management Module event log for any events related to the fan modules, and solve those events.
2. Check the ambient room temperature to ensure that the room is not too hot.
3. Check for any blockage on or near the ventilation holes on the chassis. Remove any blockages that you find.
4. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that nothing is covering the bays. Empty bays can cause a reduction in airflow to the devices in the chassis.
5. Check the ambient chassis temperature. Make sure that enough fan modules are installed to sufficiently cool the devices in the chassis. See the chassis documentation to determine how many fan modules should be installed.
6. Check the status of the specified power supply. If the internal fan has failed, replace the power supply.

- **0821E001 : Hardware removed from [arg1].**

  Hardware has been removed from the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0101

  User Response
  Information only; no action is required.

- **0821E002 : Hardware removed from [arg1].**

  Hardware has been removed from the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

Alert Category
Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0101

User Response
Information only; no action is required.

- **0821E003 : Hardware removed from [arg1].**

  Hardware has been removed from the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0101

  User Response
  Information only; no action is required.

- **0821E004 : Hardware removed from [arg1].**

  Hardware has been removed from the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0101

  User Response
  Information only; no action is required.

- **0821E005 : Hardware removed from [arg1].**

  Hardware has been removed from the specified bay in the chassis.

  Severity

Informational

Serviceable
No

Automatically notify support
No

Alert Category
Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0101

User Response
Information only; no action is required.

- **0821E006 : Hardware removed from [arg1].**

  Hardware has been removed from the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0101

  User Response
  Information only; no action is required.

- **08236001 : Power supply [arg1] has shut down because of an overcurrent fault.**

  The power current of the specified power supply has exceeded the current fault threshold, and the power supply has shut down.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Critical)

  SNMP Trap ID
  mmTrapPsC

  CIM Information

Prefix: CMM **ID:** 0028

User Response
Replace the power supply.

- **08236002 : Power supply [arg1] has shut down because of an overcurrent fault.**

  The power current of the specified power supply has exceeded the current fault threshold, and the power supply has shut down.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Critical)

  SNMP Trap ID
  mmTrapPsC

  CIM Information
  Prefix: CMM **ID:** 0028

  User Response
  Replace the power supply.

- **08236003 : Power supply [arg1] has shut down because of an overcurrent fault.**

  The power current of the specified power supply has exceeded the current fault threshold, and the power supply has shut down.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Critical)

  SNMP Trap ID
  mmTrapPsC

  CIM Information
  Prefix: CMM **ID:** 0028

  User Response
  Replace the power supply.

- **08236004 : Power supply [arg1] has shut down because of an overcurrent fault.**

  The power current of the specified power supply has exceeded the current fault threshold, and the power supply has shut down.

  Severity
  Error

  Serviceable

Yes

Automatically notify support
Yes

Alert Category
Power Modules (Critical)

SNMP Trap ID
mmTrapPsC

CIM Information
Prefix: CMM **ID:** 0028

User Response
Replace the power supply.

- **08236005 : Power supply [arg1] has shut down because of an overcurrent fault.**

  The power current of the specified power supply has exceeded the current fault threshold, and the power supply has shut down.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Critical)

  SNMP Trap ID
  mmTrapPsC

  CIM Information
  Prefix: CMM **ID:** 0028

  User Response
  Replace the power supply.

- **08236006 : Power supply [arg1] has shut down because of an overcurrent fault.**

  The power current of the specified power supply has exceeded the current fault threshold, and the power supply has shut down.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Critical)

  SNMP Trap ID
  mmTrapPsC

  CIM Information
  Prefix: CMM **ID:** 0028

User Response
Replace the power supply.

- **08236481 : Power supply [arg1] has shut down because of an overvoltage fault.**

  The voltage output of the specified power supply exceeds +12 V, and the power supply has shut down.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Critical)

  SNMP Trap ID
  mmTrapPsC

  CIM Information
  Prefix: CMM **ID:** 0026

  User Response
  Replace the power supply.

- **08236482 : Power supply [arg1] has shut down because of an overvoltage fault.**

  The voltage output of the specified power supply exceeds +12 V, and the power supply has shut down.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Critical)

  SNMP Trap ID
  mmTrapPsC

  CIM Information
  Prefix: CMM **ID:** 0026

  User Response
  Replace the power supply.

- **08236483 : Power supply [arg1] has shut down because of an overvoltage fault.**

  The voltage output of the specified power supply exceeds +12 V, and the power supply has shut down.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category

Power Modules (Critical)

SNMP Trap ID
mmTrapPsC

CIM Information
Prefix: CMM **ID:** 0026

User Response
Replace the power supply.

- **08236484 : Power supply [arg1] has shut down because of an overvoltage fault.**

The voltage output of the specified power supply exceeds +12 V, and the power supply has shut down.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Power Modules (Critical)

SNMP Trap ID
mmTrapPsC

CIM Information
Prefix: CMM **ID:** 0026

User Response
Replace the power supply.

- **08236485 : Power supply [arg1] has shut down because of an overvoltage fault.**

The voltage output of the specified power supply exceeds +12 V, and the power supply has shut down.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Power Modules (Critical)

SNMP Trap ID
mmTrapPsC

CIM Information
Prefix: CMM **ID:** 0026

User Response
Replace the power supply.

- **08236486 : Power supply [arg1] has shut down because of an overvoltage fault.**

The voltage output of the specified power supply exceeds +12 V, and the power supply has shut down.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Power Modules (Critical)

SNMP Trap ID
mmTrapPsC

CIM Information
Prefix: CMM **ID:** 0026

User Response
Replace the power supply.

- **08236801 : Power supply [arg1] has shut down because of an undervoltage fault.**

  The voltage output of the specified power supply has dropped below the voltage tolerance, and the power supply has shut down.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Critical)

  SNMP Trap ID
  mmTrapPsC

  CIM Information
  Prefix: CMM **ID:** 0027

  User Response
  Replace the power supply.

- **08236802 : Power supply [arg1] has shut down because of an undervoltage fault.**

  The voltage output of the specified power supply has dropped below the voltage tolerance, and the power supply has shut down.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Critical)

  SNMP Trap ID
  mmTrapPsC

  CIM Information
  Prefix: CMM **ID:** 0027

User Response
Replace the power supply.

- **08236803 : Power supply [arg1] has shut down because of an undervoltage fault.**

  The voltage output of the specified power supply has dropped below the voltage tolerance, and the power supply has shut down.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Critical)

  SNMP Trap ID
  mmTrapPsC

  CIM Information
  Prefix: CMM **ID:** 0027

  User Response
  Replace the power supply.

- **08236804 : Power supply [arg1] has shut down because of an undervoltage fault.**

  The voltage output of the specified power supply has dropped below the voltage tolerance, and the power supply has shut down.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Critical)

  SNMP Trap ID
  mmTrapPsC

  CIM Information
  Prefix: CMM **ID:** 0027

  User Response
  Replace the power supply.

- **08236805 : Power supply [arg1] has shut down because of an undervoltage fault.**

  The voltage output of the specified power supply has dropped below the voltage tolerance, and the power supply has shut down.

  Severity
  Error

  Serviceable
  Yes

Automatically notify support
Yes

Alert Category
Power Modules (Critical)

SNMP Trap ID
mmTrapPsC

CIM Information
Prefix: CMM **ID:** 0027

User Response
Replace the power supply.

- **08236806 : Power supply [arg1] has shut down because of an undervoltage fault.**

  The voltage output of the specified power supply has dropped below the voltage tolerance, and the power supply has shut down.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Critical)

  SNMP Trap ID
  mmTrapPsC

  CIM Information
  Prefix: CMM **ID:** 0027

  User Response
  Replace the power supply.

- **08526001 : Power supply [arg1] encountered an internal fan failure.**

  A power supply contains two internal fans that cool the power supply. The specified power supply has reported an internal fan failure, which might cause the power supply to shut down.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Critical)

  SNMP Trap ID
  mmTrapPsC

  CIM Information
  Prefix: CMM **ID:** 0039

  User Response
  Replace the power supply.

- **08526002 : Power supply [arg1] encountered an internal fan failure.**

  A power supply contains two internal fans that cool the power supply. The specified power supply has reported an internal fan failure, which might cause the power supply to shut down.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Critical)

  SNMP Trap ID
  mmTrapPsC

  CIM Information
  Prefix: CMM **ID:** 0039

  User Response
  Replace the power supply.
- **08526003 : Power supply [arg1] encountered an internal fan failure.**

  A power supply contains two internal fans that cool the power supply. The specified power supply has reported an internal fan failure, which might cause the power supply to shut down.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Critical)

  SNMP Trap ID
  mmTrapPsC

  CIM Information
  Prefix: CMM **ID:** 0039

  User Response
  Replace the power supply.
- **08526004 : Power supply [arg1] encountered an internal fan failure.**

  A power supply contains two internal fans that cool the power supply. The specified power supply has reported an internal fan failure, which might cause the power supply to shut down.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

Alert Category
Power Modules (Critical)

SNMP Trap ID
mmTrapPsC

CIM Information
Prefix: CMM **ID:** 0039

User Response
Replace the power supply.

- **08526005 : Power supply [arg1] encountered an internal fan failure.**

  A power supply contains two internal fans that cool the power supply. The specified power supply has reported an internal fan failure, which might cause the power supply to shut down.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Critical)

  SNMP Trap ID
  mmTrapPsC

  CIM Information
  Prefix: CMM **ID:** 0039

  User Response
  Replace the power supply.

- **08526006 : Power supply [arg1] encountered an internal fan failure.**

  A power supply contains two internal fans that cool the power supply. The specified power supply has reported an internal fan failure, which might cause the power supply to shut down.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Critical)

  SNMP Trap ID
  mmTrapPsC

  CIM Information
  Prefix: CMM **ID:** 0039

  User Response
  Replace the power supply.

- **08556001 : An internal fan in power supply [arg1] is operating outside the recommended speed.**

A power supply contains two internal fans that cool the power supply. One of the fans in the specified power supply is operating outside of the normal speed range. This is a Predictive Failure Analysis (PFA) event that indicates the potential for a power-supply failure.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Power Modules (Warning)

SNMP Trap ID
mmTrapPowerN

CIM Information
Prefix: CMM **ID:** 0041

User Response
At the next scheduled maintenance opportunity, replace the specified power supply.

- **08556002 : An internal fan in power supply [arg1] is operating outside the recommended speed.**

A power supply contains two internal fans that cool the power supply. One of the fans in the specified power supply is operating outside of the normal speed range. This is a Predictive Failure Analysis (PFA) event that indicates the potential for a power-supply failure.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Power Modules (Warning)

SNMP Trap ID
mmTrapPowerN

CIM Information
Prefix: CMM **ID:** 0041

User Response
At the next scheduled maintenance opportunity, replace the specified power supply.

- **08556003 : An internal fan in power supply [arg1] is operating outside the recommended speed.**

A power supply contains two internal fans that cool the power supply. One of the fans in the specified power supply is operating outside of the normal speed range. This is a Predictive Failure Analysis (PFA) event that indicates the potential for a power-supply failure.

Severity
Warning

Serviceable
Yes

Automatically notify support

Yes

Alert Category
Power Modules (Warning)

SNMP Trap ID
mmTrapPowerN

CIM Information
Prefix: CMM **ID:** 0041

User Response
At the next scheduled maintenance opportunity, replace the specified power supply.

- **08556004 : An internal fan in power supply [arg1] is operating outside the recommended speed.**

  A power supply contains two internal fans that cool the power supply. One of the fans in the specified power supply is operating outside of the normal speed range. This is a Predictive Failure Analysis (PFA) event that indicates the potential for a power-supply failure.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Warning)

  SNMP Trap ID
  mmTrapPowerN

  CIM Information
  Prefix: CMM **ID:** 0041

  User Response
  At the next scheduled maintenance opportunity, replace the specified power supply.

- **08556005 : An internal fan in power supply [arg1] is operating outside the recommended speed.**

  A power supply contains two internal fans that cool the power supply. One of the fans in the specified power supply is operating outside of the normal speed range. This is a Predictive Failure Analysis (PFA) event that indicates the potential for a power-supply failure.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Warning)

  SNMP Trap ID
  mmTrapPowerN

  CIM Information
  Prefix: CMM **ID:** 0041

  User Response

At the next scheduled maintenance opportunity, replace the specified power supply.

- **08556006 : An internal fan in power supply [arg1] is operating outside the recommended speed.**

  A power supply contains two internal fans that cool the power supply. One of the fans in the specified power supply is operating outside of the normal speed range. This is a Predictive Failure Analysis (PFA) event that indicates the potential for a power-supply failure.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Power Modules (Warning)

  SNMP Trap ID
  mmTrapPowerN

  CIM Information
  Prefix: CMM **ID:** 0041

  User Response
  At the next scheduled maintenance opportunity, replace the specified power supply.

- **0901E000 : Chassis front LED card not present.**

  The front LED card was not detected. The card is attached internally via a ribbon cable to the front of the chassis. If the front LED card is disconnected, the LEDs on the front information panel will not work. The chassis LED status is available via the user interface.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0022

  User Response
  Install or replace the front LED card. Make sure that the front LED card is connected after a maintenance action.

- **0901E003 : Chassis rear LED card not present.**

  The rear LED card was not detected. Warranty information and chassis vital product data (VPD) are stored on the rear LED card. If the rear LED card is disconnected, it cannot correctly identify the chassis type, and the chassis LEDs will not work.

  Severity
  Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Chassis/System Management (Critical)

SNMP Trap ID
mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0060

User Response
Install or replace the rear LED card. Note that you must remove power from the chassis for this action.

- **0A002001 : Hardware inserted in [arg1].**

Hardware has been installed in the specified bay in the chassis.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0100

User Response
Information only; no action is required.

- **0A002002 : Hardware inserted in [arg1].**

Hardware has been installed in the specified bay in the chassis.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0100

User Response
Information only; no action is required.

- **0A002003 : Hardware inserted in [arg1].**

  Hardware has been installed in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0100

  User Response
  Information only; no action is required.

- **0A002004 : Hardware inserted in [arg1].**

  Hardware has been installed in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0100

  User Response
  Information only; no action is required.

- **0A002005 : Hardware inserted in [arg1].**

  Hardware has been installed in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category

Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0100

User Response
Information only; no action is required.

- **0A002006 : Hardware inserted in [arg1].**

  Hardware has been installed in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0100

  User Response
  Information only; no action is required.

- **0A002007 : Hardware inserted in [arg1].**

  Hardware has been installed in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0100

  User Response
  Information only; no action is required.

- **0A002008 : Hardware inserted in [arg1].**

  Hardware has been installed in the specified bay in the chassis.

  Severity
  Informational

Serviceable
No

Automatically notify support
No

Alert Category
Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0100

User Response
Information only; no action is required.

- **0A002009 : Hardware inserted in [arg1].**

Hardware has been installed in the specified bay in the chassis.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0100

User Response
Information only; no action is required.

- **0A00200A : Hardware inserted in [arg1].**

Hardware has been installed in the specified bay in the chassis.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0100

User Response

Information only; no action is required.

- **0A002101 : Failed to discover device [arg1] in [arg2].**

  Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0103

  User Response
  Information only; no action is required.

- **0A002102 : Failed to discover device [arg1] in [arg2].**

  Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0103

  User Response
  Information only; no action is required.

- **0A002103 : Failed to discover device [arg1] in [arg2].**

  Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support

No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0103

User Response
Information only; no action is required.

- **0A002104 : Failed to discover device [arg1] in [arg2].**

  Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0103

  User Response
  Information only; no action is required.

- **0A002105 : Failed to discover device [arg1] in [arg2].**

  Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0103

  User Response
  Information only; no action is required.

- **0A002106 : Failed to discover device [arg1] in [arg2].**

Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0103

User Response
Information only; no action is required.

- **0A002107 : Failed to discover device [arg1] in [arg2].**

  Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0103

  User Response
  Information only; no action is required.

- **0A002108 : Failed to discover device [arg1] in [arg2].**

  Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category

Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0103

User Response
Information only; no action is required.

- **0A002109 : Failed to discover device [arg1] in [arg2].**

  Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0103

  User Response
  Information only; no action is required.

- **0A00210A : Failed to discover device [arg1] in [arg2].**

  Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0103

  User Response
  Information only; no action is required.

- **0A003001 : Hardware removed from [arg1].**

  Hardware has been removed from the specified bay in the chassis.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0101

User Response
Information only; no action is required.

- **0A003002 : Hardware removed from [arg1].**

  Hardware has been removed from the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0101

  User Response
  Information only; no action is required.

- **0A003003 : Hardware removed from [arg1].**

  Hardware has been removed from the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information

Prefix: CMM **ID:** 0101

User Response
Information only; no action is required.

- **0A003004 : Hardware removed from [arg1].**

  Hardware has been removed from the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0101

  User Response
  Information only; no action is required.

- **0A003005 : Hardware removed from [arg1].**

  Hardware has been removed from the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0101

  User Response
  Information only; no action is required.

- **0A003006 : Hardware removed from [arg1].**

  Hardware has been removed from the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

Alert Category
Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0101

User Response
Information only; no action is required.

- **0A003007 : Hardware removed from [arg1].**

  Hardware has been removed from the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0101

  User Response
  Information only; no action is required.

- **0A003008 : Hardware removed from [arg1].**

  Hardware has been removed from the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0101

  User Response
  Information only; no action is required.

- **0A003009 : Hardware removed from [arg1].**

  Hardware has been removed from the specified bay in the chassis.

  Severity

Informational

Serviceable
No

Automatically notify support
No

Alert Category
Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0101

User Response
Information only; no action is required.

- **0A00300A : Hardware removed from [arg1].**

  Hardware has been removed from the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0101

  User Response
  Information only; no action is required.

- **0A003101 : Discovered device [arg1] in [arg2], CRC: [arg3].**

  Hardware has been discovered successfully in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0102

User Response
Information only; no action is required.

- **0A003102 : Discovered device [arg1] in [arg2], CRC: [arg3].**

  Hardware has been discovered successfully in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0102

  User Response
  Information only; no action is required.

- **0A003103 : Discovered device [arg1] in [arg2], CRC: [arg3].**

  Hardware has been discovered successfully in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0102

  User Response
  Information only; no action is required.

- **0A003104 : Discovered device [arg1] in [arg2], CRC: [arg3].**

  Hardware has been discovered successfully in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category

Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0102

User Response
Information only; no action is required.

- **0A003105 : Discovered device [arg1] in [arg2], CRC: [arg3].**

  Hardware has been discovered successfully in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0102

  User Response
  Information only; no action is required.

- **0A003106 : Discovered device [arg1] in [arg2], CRC: [arg3].**

  Hardware has been discovered successfully in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0102

  User Response
  Information only; no action is required.

- **0A003107 : Discovered device [arg1] in [arg2], CRC: [arg3].**

  Hardware has been discovered successfully in the specified bay in the chassis.

  Severity
  Informational

Serviceable
No

Automatically notify support
No

Alert Category
Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0102

User Response
Information only; no action is required.

- **0A003108 : Discovered device [arg1] in [arg2], CRC: [arg3].**

Hardware has been discovered successfully in the specified bay in the chassis.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0102

User Response
Information only; no action is required.

- **0A003109 : Discovered device [arg1] in [arg2], CRC: [arg3].**

Hardware has been discovered successfully in the specified bay in the chassis.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0102

User Response

Information only; no action is required.

- **0A00310A : Discovered device [arg1] in [arg2], CRC: [arg3].**

  Hardware has been discovered successfully in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0102

  User Response
  Information only; no action is required.

- **0E002001 : Hardware inserted in [arg1].**

  Hardware has been installed in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0100

  User Response
  Information only; no action is required.

- **0E002002 : Hardware inserted in [arg1].**

  Hardware has been installed in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0100

User Response
Information only; no action is required.

- **0E002003 : Hardware inserted in [arg1].**

  Hardware has been installed in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0100

  User Response
  Information only; no action is required.

- **0E002004 : Hardware inserted in [arg1].**

  Hardware has been installed in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0100

  User Response
  Information only; no action is required.

- **0E002005 : Hardware inserted in [arg1].**

  Hardware has been installed in the specified bay in the chassis.

  Severity
  Informational

  Serviceable

No

Automatically notify support
No

Alert Category
Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0100

User Response
Information only; no action is required.

- **0E002006 : Hardware inserted in [arg1].**

Hardware has been installed in the specified bay in the chassis.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0100

User Response
Information only; no action is required.

- **0E002007 : Hardware inserted in [arg1].**

Hardware has been installed in the specified bay in the chassis.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0100

User Response
Information only; no action is required.

- **0E002008 : Hardware inserted in [arg1].**

  Hardware has been installed in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0100

  User Response
  Information only; no action is required.
- **0E002009 : Hardware inserted in [arg1].**

  Hardware has been installed in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0100

  User Response
  Information only; no action is required.
- **0E00200A : Hardware inserted in [arg1].**

  Hardware has been installed in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0100

User Response
Information only; no action is required.

- **0E00200B : Hardware inserted in [arg1].**

  Hardware has been installed in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0100

  User Response
  Information only; no action is required.

- **0E00200C : Hardware inserted in [arg1].**

  Hardware has been installed in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0100

  User Response
  Information only; no action is required.

- **0E00200D : Hardware inserted in [arg1].**

  Hardware has been installed in the specified bay in the chassis.

  Severity
  Informational

  Serviceable

No

Automatically notify support
No

Alert Category
Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0100

User Response
Information only; no action is required.

- **0E00200E : Hardware inserted in [arg1].**

  Hardware has been installed in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0100

  User Response
  Information only; no action is required.

- **0E002101 : Discovered device [arg1] in [arg2], CRC: [arg3].**

  Hardware has been discovered successfully in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0102

  User Response
  Information only; no action is required.

- **0E002102 : Discovered device [arg1] in [arg2], CRC: [arg3].**

  Hardware has been discovered successfully in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0102

  User Response
  Information only; no action is required.
- **0E002103 : Discovered device [arg1] in [arg2], CRC: [arg3].**

  Hardware has been discovered successfully in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0102

  User Response
  Information only; no action is required.
- **0E002104 : Discovered device [arg1] in [arg2], CRC: [arg3].**

  Hardware has been discovered successfully in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0102

User Response
Information only; no action is required.

- **0E002105 : Discovered device [arg1] in [arg2], CRC: [arg3].**

  Hardware has been discovered successfully in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0102

  User Response
  Information only; no action is required.

- **0E002106 : Discovered device [arg1] in [arg2], CRC: [arg3].**

  Hardware has been discovered successfully in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0102

  User Response
  Information only; no action is required.

- **0E002107 : Discovered device [arg1] in [arg2], CRC: [arg3].**

  Hardware has been discovered successfully in the specified bay in the chassis.

  Severity
  Informational

  Serviceable

No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0102

User Response
Information only; no action is required.

- **0E002108 : Discovered device [arg1] in [arg2], CRC: [arg3].**

Hardware has been discovered successfully in the specified bay in the chassis.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0102

User Response
Information only; no action is required.

- **0E002109 : Discovered device [arg1] in [arg2], CRC: [arg3].**

Hardware has been discovered successfully in the specified bay in the chassis.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0102

User Response
Information only; no action is required.

- **0E00210A : Discovered device [arg1] in [arg2], CRC: [arg3].**

  Hardware has been discovered successfully in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0102

  User Response
  Information only; no action is required.
- **0E00210B : Discovered device [arg1] in [arg2], CRC: [arg3].**

  Hardware has been discovered successfully in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0102

  User Response
  Information only; no action is required.
- **0E00210C : Discovered device [arg1] in [arg2], CRC: [arg3].**

  Hardware has been discovered successfully in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0102

User Response
Information only; no action is required.

- **0E00210D : Discovered device [arg1] in [arg2], CRC: [arg3].**

  Hardware has been discovered successfully in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0102

  User Response
  Information only; no action is required.

- **0E00210E : Discovered device [arg1] in [arg2], CRC: [arg3].**

  Hardware has been discovered successfully in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0102

  User Response
  Information only; no action is required.

- **0E002201 : Failed to discover device [arg1] in [arg2].**

  Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

  Severity
  Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0103

User Response
Information only; no action is required.

- **0E002202 : Failed to discover device [arg1] in [arg2].**

  Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0103

  User Response
  Information only; no action is required.

- **0E002203 : Failed to discover device [arg1] in [arg2].**

  Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0103

User Response
Information only; no action is required.

- **0E002204 : Failed to discover device [arg1] in [arg2].**

  Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0103

  User Response
  Information only; no action is required.

- **0E002205 : Failed to discover device [arg1] in [arg2].**

  Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0103

  User Response
  Information only; no action is required.

- **0E002206 : Failed to discover device [arg1] in [arg2].**

  Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

  Severity
  Informational

  Serviceable
  No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0103

User Response
Information only; no action is required.

- **0E002207 : Failed to discover device [arg1] in [arg2].**

  Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0103

  User Response
  Information only; no action is required.

- **0E002208 : Failed to discover device [arg1] in [arg2].**

  Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0103

  User Response
  Information only; no action is required.

- **0E002209 : Failed to discover device [arg1] in [arg2].**

  Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0103

  User Response
  Information only; no action is required.
- **0E00220A : Failed to discover device [arg1] in [arg2].**

  Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0103

  User Response
  Information only; no action is required.
- **0E00220B : Failed to discover device [arg1] in [arg2].**

  Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0103

User Response
Information only; no action is required.

- **0E00220C : Failed to discover device [arg1] in [arg2].**

  Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0103

  User Response
  Information only; no action is required.

- **0E00220D : Failed to discover device [arg1] in [arg2].**

  Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0103

  User Response
  Information only; no action is required.

- **0E00220E : Failed to discover device [arg1] in [arg2].**

Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0103

User Response
Information only; no action is required.

- **0E004001 : Hardware removed from [arg1].**

Hardware has been removed from the specified bay in the chassis.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0101

User Response
Information only; no action is required.

- **0E004002 : Hardware removed from [arg1].**

Hardware has been removed from the specified bay in the chassis.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Inventory change (Informational)

SNMP Trap ID

mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0101

User Response
Information only; no action is required.

- **0E004003 : Hardware removed from [arg1].**

  Hardware has been removed from the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0101

  User Response
  Information only; no action is required.

- **0E004004 : Hardware removed from [arg1].**

  Hardware has been removed from the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0101

  User Response
  Information only; no action is required.

- **0E004005 : Hardware removed from [arg1].**

  Hardware has been removed from the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

Automatically notify support
No

Alert Category
Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0101

User Response
Information only; no action is required.

- **0E004006 : Hardware removed from [arg1].**

Hardware has been removed from the specified bay in the chassis.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0101

User Response
Information only; no action is required.

- **0E004007 : Hardware removed from [arg1].**

Hardware has been removed from the specified bay in the chassis.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0101

User Response
Information only; no action is required.

- **0E004008 : Hardware removed from [arg1].**

Hardware has been removed from the specified bay in the chassis.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0101

User Response
Information only; no action is required.

- **0E004009 : Hardware removed from [arg1].**

Hardware has been removed from the specified bay in the chassis.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0101

User Response
Information only; no action is required.

- **0E00400A : Hardware removed from [arg1].**

Hardware has been removed from the specified bay in the chassis.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0101

User Response
Information only; no action is required.

- **0E00400B : Hardware removed from [arg1].**

  Hardware has been removed from the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0101

  User Response
  Information only; no action is required.

- **0E00400C : Hardware removed from [arg1].**

  Hardware has been removed from the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0101

  User Response
  Information only; no action is required.

- **0E00400D : Hardware removed from [arg1].**

  Hardware has been removed from the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support

No

Alert Category
Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0101

User Response
Information only; no action is required.

- **0E00400E : Hardware removed from [arg1].**

  Hardware has been removed from the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0101

  User Response
  Information only; no action is required.

- **0E006001 : Node [arg1] incompatible with the I/O-module configuration.**

  The fabric type of an expansion card in the specified node is not compatible with an I/O module in the I/O bay. Data might not be passed on one or more possible connections.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0020

  User Response
  Make sure that the network is set up correctly. If the network configuration is correct, no action is required. Otherwise, make sure that the fabric type of the expansion card in the specified node is compatible with the fabric type of the I/O module.

- **0E006002 : Node [arg1] incompatible with the I/O-module configuration.**

  The fabric type of an expansion card in the specified node is not compatible with an I/O module in the I/O bay. Data might not be passed on one or more possible connections.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0020

  User Response
  Make sure that the network is set up correctly. If the network configuration is correct, no action is required. Otherwise, make sure that the fabric type of the expansion card in the specified node is compatible with the fabric type of the I/O module.
- **0E006003 : Node [arg1] incompatible with the I/O-module configuration.**

  The fabric type of an expansion card in the specified node is not compatible with an I/O module in the I/O bay. Data might not be passed on one or more possible connections.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0020

  User Response
  Make sure that the network is set up correctly. If the network configuration is correct, no action is required. Otherwise, make sure that the fabric type of the expansion card in the specified node is compatible with the fabric type of the I/O module.
- **0E006004 : Node [arg1] incompatible with the I/O-module configuration.**

  The fabric type of an expansion card in the specified node is not compatible with an I/O module in the I/O bay. Data might not be passed on one or more possible connections.

  Severity
  Warning

  Serviceable

Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0020

User Response
Make sure that the network is set up correctly. If the network configuration is correct, no action is required. Otherwise, make sure that the fabric type of the expansion card in the specified node is compatible with the fabric type of the I/O module.

- **0E006005 : Node [arg1] incompatible with the I/O-module configuration.**

The fabric type of an expansion card in the specified node is not compatible with an I/O module in the I/O bay. Data might not be passed on one or more possible connections.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0020

User Response
Make sure that the network is set up correctly. If the network configuration is correct, no action is required. Otherwise, make sure that the fabric type of the expansion card in the specified node is compatible with the fabric type of the I/O module.

- **0E006006 : Node [arg1] incompatible with the I/O-module configuration.**

The fabric type of an expansion card in the specified node is not compatible with an I/O module in the I/O bay. Data might not be passed on one or more possible connections.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID

mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0020

User Response
Make sure that the network is set up correctly. If the network configuration is correct, no action is required. Otherwise, make sure that the fabric type of the expansion card in the specified node is compatible with the fabric type of the I/O module.

- **0E006007 : Node [arg1] incompatible with the I/O-module configuration.**

The fabric type of an expansion card in the specified node is not compatible with an I/O module in the I/O bay. Data might not be passed on one or more possible connections.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0020

User Response
Make sure that the network is set up correctly. If the network configuration is correct, no action is required. Otherwise, make sure that the fabric type of the expansion card in the specified node is compatible with the fabric type of the I/O module.

- **0E006008 : Node [arg1] incompatible with the I/O-module configuration.**

The fabric type of an expansion card in the specified node is not compatible with an I/O module in the I/O bay. Data might not be passed on one or more possible connections.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0020

User Response
Make sure that the network is set up correctly. If the network configuration is correct, no action is required. Otherwise, make sure that the fabric type of the expansion card in the specified node is compatible with the fabric type of the I/O module.

- **0E006009 : Node [arg1] incompatible with the I/O-module configuration.**

  The fabric type of an expansion card in the specified node is not compatible with an I/O module in the I/O bay. Data might not be passed on one or more possible connections.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0020

  User Response
  Make sure that the network is set up correctly. If the network configuration is correct, no action is required. Otherwise, make sure that the fabric type of the expansion card in the specified node is compatible with the fabric type of the I/O module.
- **0E00600A : Node [arg1] incompatible with the I/O-module configuration.**

  The fabric type of an expansion card in the specified node is not compatible with an I/O module in the I/O bay. Data might not be passed on one or more possible connections.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0020

  User Response
  Make sure that the network is set up correctly. If the network configuration is correct, no action is required. Otherwise, make sure that the fabric type of the expansion card in the specified node is compatible with the fabric type of the I/O module.
- **0E00600B : Node [arg1] incompatible with the I/O-module configuration.**

  The fabric type of an expansion card in the specified node is not compatible with an I/O module in the I/O bay. Data might not be passed on one or more possible connections.

  Severity
  Warning

  Serviceable

Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0020

User Response
Make sure that the network is set up correctly. If the network configuration is correct, no action is required. Otherwise, make sure that the fabric type of the expansion card in the specified node is compatible with the fabric type of the I/O module.

- **0E00600C : Node [arg1] incompatible with the I/O-module configuration.**

The fabric type of an expansion card in the specified node is not compatible with an I/O module in the I/O bay. Data might not be passed on one or more possible connections.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0020

User Response
Make sure that the network is set up correctly. If the network configuration is correct, no action is required. Otherwise, make sure that the fabric type of the expansion card in the specified node is compatible with the fabric type of the I/O module.

- **0E00600D : Node [arg1] incompatible with the I/O-module configuration.**

The fabric type of an expansion card in the specified node is not compatible with an I/O module in the I/O bay. Data might not be passed on one or more possible connections.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID

mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0020

User Response
Make sure that the network is set up correctly. If the network configuration is correct, no action is required. Otherwise, make sure that the fabric type of the expansion card in the specified node is compatible with the fabric type of the I/O module.

- **0E00600E : Node [arg1] incompatible with the I/O-module configuration.**

The fabric type of an expansion card in the specified node is not compatible with an I/O module in the I/O bay. Data might not be passed on one or more possible connections.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0020

User Response
Make sure that the network is set up correctly. If the network configuration is correct, no action is required. Otherwise, make sure that the fabric type of the expansion card in the specified node is compatible with the fabric type of the I/O module.

- **0E008001 : The system-management processor for [arg1] communication to the CMM is offline.**

The specified node is not responding to the Chassis Management Module (CMM) on the node-management bus. The node operating system and devices might be working, but there is no monitoring capability from the CMM.

Severity
Error

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0098

User Response
Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.
4. Log in to the system-management processor directly if a user interface is supported, and reset the system-management processor.
5. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **0E008002 : The system-management processor for [arg1] communication to the CMM is offline.**

  The specified node is not responding to the Chassis Management Module (CMM) on the node-management bus. The node operating system and devices might be working, but there is no monitoring capability from the CMM.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Critical)

  SNMP Trap ID
  mmTrapBladeC

  CIM Information
  Prefix: CMM **ID:** 0098

  User Response
  Complete the following steps until the problem is solved:

  1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
  2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
  3. Perform a hard restart of the node system-management processor.
  4. Log in to the system-management processor directly if a user interface is supported, and reset the system-management processor.
  5. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **0E008003 : The system-management processor for [arg1] communication to the CMM is offline.**

  The specified node is not responding to the Chassis Management Module (CMM) on the node-management bus. The node operating system and devices might be working, but there is no monitoring capability from the CMM.

Severity
Error

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0098

User Response
Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.
4. Log in to the system-management processor directly if a user interface is supported, and reset the system-management processor.
5. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **0E008004 : The system-management processor for [arg1] communication to the CMM is offline.**

The specified node is not responding to the Chassis Management Module (CMM) on the node-management bus. The node operating system and devices might be working, but there is no monitoring capability from the CMM.

Severity
Error

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0098

User Response
Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.
4. Log in to the system-management processor directly if a user interface is supported, and reset the system-management processor.
5. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **0E008005 : The system-management processor for [arg1] communication to the CMM is offline.**

  The specified node is not responding to the Chassis Management Module (CMM) on the node-management bus. The node operating system and devices might be working, but there is no monitoring capability from the CMM.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Critical)

  SNMP Trap ID
  mmTrapBladeC

  CIM Information
  Prefix: CMM **ID:** 0098

  User Response
  Complete the following steps until the problem is solved:

  1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
  2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
  3. Perform a hard restart of the node system-management processor.
  4. Log in to the system-management processor directly if a user interface is supported, and reset the system-management processor.
  5. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **0E008006 : The system-management processor for [arg1] communication to the CMM is offline.**

  The specified node is not responding to the Chassis Management Module (CMM) on the node-management bus. The node operating system and devices might be working, but there is no monitoring capability from the CMM.

Severity
Error

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0098

User Response
Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.
4. Log in to the system-management processor directly if a user interface is supported, and reset the system-management processor.
5. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **0E008007 : The system-management processor for [arg1] communication to the CMM is offline.**

The specified node is not responding to the Chassis Management Module (CMM) on the node-management bus. The node operating system and devices might be working, but there is no monitoring capability from the CMM.

Severity
Error

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0098

User Response
Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.
4. Log in to the system-management processor directly if a user interface is supported, and reset the system-management processor.
5. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **0E008008 : The system-management processor for [arg1] communication to the CMM is offline.**

  The specified node is not responding to the Chassis Management Module (CMM) on the node-management bus. The node operating system and devices might be working, but there is no monitoring capability from the CMM.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Critical)

  SNMP Trap ID
  mmTrapBladeC

  CIM Information
  Prefix: CMM **ID:** 0098

  User Response
  Complete the following steps until the problem is solved:

  1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
  2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
  3. Perform a hard restart of the node system-management processor.
  4. Log in to the system-management processor directly if a user interface is supported, and reset the system-management processor.
  5. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **0E008009 : The system-management processor for [arg1] communication to the CMM is offline.**

  The specified node is not responding to the Chassis Management Module (CMM) on the node-management bus. The node operating system and devices might be working, but there is no monitoring capability from the CMM.

Severity
Error

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0098

User Response
Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.
4. Log in to the system-management processor directly if a user interface is supported, and reset the system-management processor.
5. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **0E00800A : The system-management processor for [arg1] communication to the CMM is offline.**

The specified node is not responding to the Chassis Management Module (CMM) on the node-management bus. The node operating system and devices might be working, but there is no monitoring capability from the CMM.

Severity
Error

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0098

User Response
Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.
4. Log in to the system-management processor directly if a user interface is supported, and reset the system-management processor.
5. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **0E00800B : The system-management processor for [arg1] communication to the CMM is offline.**

  The specified node is not responding to the Chassis Management Module (CMM) on the node-management bus. The node operating system and devices might be working, but there is no monitoring capability from the CMM.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Critical)

  SNMP Trap ID
  mmTrapBladeC

  CIM Information
  Prefix: CMM **ID:** 0098

  User Response
  Complete the following steps until the problem is solved:

  1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
  2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
  3. Perform a hard restart of the node system-management processor.
  4. Log in to the system-management processor directly if a user interface is supported, and reset the system-management processor.
  5. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **0E00800C : The system-management processor for [arg1] communication to the CMM is offline.**

  The specified node is not responding to the Chassis Management Module (CMM) on the node-management bus. The node operating system and devices might be working, but there is no monitoring capability from the CMM.

Severity
Error

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0098

User Response
Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.
4. Log in to the system-management processor directly if a user interface is supported, and reset the system-management processor.
5. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **0E00800D : The system-management processor for [arg1] communication to the CMM is offline.**

The specified node is not responding to the Chassis Management Module (CMM) on the node-management bus. The node operating system and devices might be working, but there is no monitoring capability from the CMM.

Severity
Error

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0098

User Response
Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.
4. Log in to the system-management processor directly if a user interface is supported, and reset the system-management processor.
5. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **0E00800E : The system-management processor for [arg1] communication to the CMM is offline.**

  The specified node is not responding to the Chassis Management Module (CMM) on the node-management bus. The node operating system and devices might be working, but there is no monitoring capability from the CMM.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Critical)

  SNMP Trap ID
  mmTrapBladeC

  CIM Information
  Prefix: CMM **ID:** 0098

  User Response
  Complete the following steps until the problem is solved:

  1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
  2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
  3. Perform a hard restart of the node system-management processor.
  4. Log in to the system-management processor directly if a user interface is supported, and reset the system-management processor.
  5. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **0E00A001 : Node [arg1] cannot power on because of insufficient power.**

  The specified node cannot power on because there is not enough power capacity in the power budget.

  Severity

Warning

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0092

User Response
Use one of the following procedures to enable the node to power on:
- Choose a different power-management policy to increase the power budget for the chassis.
- Install additional power supplies to increase power capacity, if empty power-supply bays are available.
- Shut down other devices in the chassis, such as nodes or I/O modules.

- **0E00A002 : Node [arg1] cannot power on because of insufficient power.**

The specified node cannot power on because there is not enough power capacity in the power budget.

Severity
Warning

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0092

User Response
Use one of the following procedures to enable the node to power on:
- Choose a different power-management policy to increase the power budget for the chassis.
- Install additional power supplies to increase power capacity, if empty power-supply bays are available.
- Shut down other devices in the chassis, such as nodes or I/O modules.

- **0E00A003 : Node [arg1] cannot power on because of insufficient power.**

The specified node cannot power on because there is not enough power capacity in the power budget.

Severity
Warning

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0092

User Response
Use one of the following procedures to enable the node to power on:
- Choose a different power-management policy to increase the power budget for the chassis.
- Install additional power supplies to increase power capacity, if empty power-supply bays are available.
- Shut down other devices in the chassis, such as nodes or I/O modules.

- **0E00A004 : Node [arg1] cannot power on because of insufficient power.**

The specified node cannot power on because there is not enough power capacity in the power budget.

Severity
Warning

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0092

User Response
Use one of the following procedures to enable the node to power on:
- Choose a different power-management policy to increase the power budget for the chassis.
- Install additional power supplies to increase power capacity, if empty power-supply bays are available.
- Shut down other devices in the chassis, such as nodes or I/O modules.

- **0E00A005 : Node [arg1] cannot power on because of insufficient power.**

The specified node cannot power on because there is not enough power capacity in the power budget.

Severity
Warning

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information

Prefix: CMM **ID:** 0092

User Response

Use one of the following procedures to enable the node to power on:

- Choose a different power-management policy to increase the power budget for the chassis.
- Install additional power supplies to increase power capacity, if empty power-supply bays are available.
- Shut down other devices in the chassis, such as nodes or I/O modules.

- **0E00A006 : Node [arg1] cannot power on because of insufficient power.**

The specified node cannot power on because there is not enough power capacity in the power budget.

Severity

Warning

Serviceable

No

Automatically notify support

No

Alert Category

Nodes (Warning)

SNMP Trap ID

mmTrapBladeN

CIM Information

Prefix: CMM **ID:** 0092

User Response

Use one of the following procedures to enable the node to power on:

- Choose a different power-management policy to increase the power budget for the chassis.
- Install additional power supplies to increase power capacity, if empty power-supply bays are available.
- Shut down other devices in the chassis, such as nodes or I/O modules.

- **0E00A007 : Node [arg1] cannot power on because of insufficient power.**

The specified node cannot power on because there is not enough power capacity in the power budget.

Severity

Warning

Serviceable

No

Automatically notify support

No

Alert Category

Nodes (Warning)

SNMP Trap ID

mmTrapBladeN

CIM Information

Prefix: CMM **ID:** 0092

User Response

Use one of the following procedures to enable the node to power on:

- Choose a different power-management policy to increase the power budget for the chassis.

  - Install additional power supplies to increase power capacity, if empty power-supply bays are available.
  - Shut down other devices in the chassis, such as nodes or I/O modules.

- **0E00A008 : Node [arg1] cannot power on because of insufficient power.**

  The specified node cannot power on because there is not enough power capacity in the power budget.

  Severity
  Warning

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0092

  User Response
  Use one of the following procedures to enable the node to power on:
  - Choose a different power-management policy to increase the power budget for the chassis.
  - Install additional power supplies to increase power capacity, if empty power-supply bays are available.
  - Shut down other devices in the chassis, such as nodes or I/O modules.

- **0E00A009 : Node [arg1] cannot power on because of insufficient power.**

  The specified node cannot power on because there is not enough power capacity in the power budget.

  Severity
  Warning

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0092

  User Response
  Use one of the following procedures to enable the node to power on:
  - Choose a different power-management policy to increase the power budget for the chassis.
  - Install additional power supplies to increase power capacity, if empty power-supply bays are available.
  - Shut down other devices in the chassis, such as nodes or I/O modules.

- **0E00A00A : Node [arg1] cannot power on because of insufficient power.**

  The specified node cannot power on because there is not enough power capacity in the power budget.

Severity
Warning

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0092

User Response
Use one of the following procedures to enable the node to power on:
- Choose a different power-management policy to increase the power budget for the chassis.
- Install additional power supplies to increase power capacity, if empty power-supply bays are available.
- Shut down other devices in the chassis, such as nodes or I/O modules.

- **0E00A00B : Node [arg1] cannot power on because of insufficient power.**

  The specified node cannot power on because there is not enough power capacity in the power budget.

  Severity
  Warning

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0092

  User Response
  Use one of the following procedures to enable the node to power on:
  - Choose a different power-management policy to increase the power budget for the chassis.
  - Install additional power supplies to increase power capacity, if empty power-supply bays are available.
  - Shut down other devices in the chassis, such as nodes or I/O modules.

- **0E00A00C : Node [arg1] cannot power on because of insufficient power.**

  The specified node cannot power on because there is not enough power capacity in the power budget.

  Severity
  Warning

  Serviceable
  No

  Automatically notify support

No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0092

User Response
Use one of the following procedures to enable the node to power on:
- Choose a different power-management policy to increase the power budget for the chassis.
- Install additional power supplies to increase power capacity, if empty power-supply bays are available.
- Shut down other devices in the chassis, such as nodes or I/O modules.

- **0E00A00D : Node [arg1] cannot power on because of insufficient power.**

The specified node cannot power on because there is not enough power capacity in the power budget.

Severity
Warning

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0092

User Response
Use one of the following procedures to enable the node to power on:
- Choose a different power-management policy to increase the power budget for the chassis.
- Install additional power supplies to increase power capacity, if empty power-supply bays are available.
- Shut down other devices in the chassis, such as nodes or I/O modules.

- **0E00A00E : Node [arg1] cannot power on because of insufficient power.**

The specified node cannot power on because there is not enough power capacity in the power budget.

Severity
Warning

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0092

User Response
Use one of the following procedures to enable the node to power on:
- Choose a different power-management policy to increase the power budget for the chassis.
- Install additional power supplies to increase power capacity, if empty power-supply bays are available.
- Shut down other devices in the chassis, such as nodes or I/O modules.

- **0E00B001 : I/O module [arg1] cannot power on because of insufficient power.**

The specified I/O module cannot power on because there is not enough power capacity in the power budget.

Severity
Warning

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Warning)

SNMP Trap ID
mmTrapION

CIM Information
Prefix: CMM **ID:** 0094

User Response
Use one of the following procedures to enable the I/O module to power on:
- Choose a different power-management policy to increase the power budget for the chassis.
- Install additional power supplies to increase power capacity, if empty power-supply bays are available.
- Shut down other devices in the chassis, such as nodes or I/O modules.

- **0E00B002 : I/O module [arg1] cannot power on because of insufficient power.**

The specified I/O module cannot power on because there is not enough power capacity in the power budget.

Severity
Warning

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Warning)

SNMP Trap ID
mmTrapION

CIM Information
Prefix: CMM **ID:** 0094

User Response

Use one of the following procedures to enable the I/O module to power on:
  - Choose a different power-management policy to increase the power budget for the chassis.
  - Install additional power supplies to increase power capacity, if empty power-supply bays are available.
  - Shut down other devices in the chassis, such as nodes or I/O modules.

- **0E00B003 : I/O module [arg1] cannot power on because of insufficient power.**

  The specified I/O module cannot power on because there is not enough power capacity in the power budget.

  Severity
  Warning

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Warning)

  SNMP Trap ID
  mmTrapION

  CIM Information
  Prefix: CMM **ID:** 0094

  User Response
  Use one of the following procedures to enable the I/O module to power on:
  - Choose a different power-management policy to increase the power budget for the chassis.
  - Install additional power supplies to increase power capacity, if empty power-supply bays are available.
  - Shut down other devices in the chassis, such as nodes or I/O modules.

- **0E00B004 : I/O module [arg1] cannot power on because of insufficient power.**

  The specified I/O module cannot power on because there is not enough power capacity in the power budget.

  Severity
  Warning

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Warning)

  SNMP Trap ID
  mmTrapION

  CIM Information
  Prefix: CMM **ID:** 0094

  User Response
  Use one of the following procedures to enable the I/O module to power on:
  - Choose a different power-management policy to increase the power budget for the chassis.
  - Install additional power supplies to increase power capacity, if empty power-supply bays are available.

– Shut down other devices in the chassis, such as nodes or I/O modules.

- **0E010001 : Node [arg1] device [arg2][[arg3]] VPD is not available.**

  The vital product data (VPD) of the specified device is not available. VPD includes information such as the serial number and part number to uniquely identify the device.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0075

  User Response
  Complete the following steps until the problem is solved:

  1. Reset the system-management processor in the node.
  2. Replace the device.

- **0E010002 : Node [arg1] device [arg2][[arg3]] VPD is not available.**

  The vital product data (VPD) of the specified device is not available. VPD includes information such as the serial number and part number to uniquely identify the device.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0075

  User Response
  Complete the following steps until the problem is solved:

  1. Reset the system-management processor in the node.
  2. Replace the device.

- **0E010003 : Node [arg1] device [arg2][[arg3]] VPD is not available.**

  The vital product data (VPD) of the specified device is not available. VPD includes information such as the serial number and part number to uniquely identify the device.

  Severity

Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0075

User Response
Complete the following steps until the problem is solved:

1. Reset the system-management processor in the node.
2. Replace the device.

- **0E010004 : Node [arg1] device [arg2][[arg3]] VPD is not available.**

The vital product data (VPD) of the specified device is not available. VPD includes information such as the serial number and part number to uniquely identify the device.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0075

User Response
Complete the following steps until the problem is solved:

1. Reset the system-management processor in the node.
2. Replace the device.

- **0E010005 : Node [arg1] device [arg2][[arg3]] VPD is not available.**

The vital product data (VPD) of the specified device is not available. VPD includes information such as the serial number and part number to uniquely identify the device.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0075

User Response
Complete the following steps until the problem is solved:

1. Reset the system-management processor in the node.
2. Replace the device.

- **0E010006 : Node [arg1] device [arg2][[arg3]] VPD is not available.**

The vital product data (VPD) of the specified device is not available. VPD includes information such as the serial number and part number to uniquely identify the device.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0075

User Response
Complete the following steps until the problem is solved:

1. Reset the system-management processor in the node.
2. Replace the device.

- **0E010007 : Node [arg1] device [arg2][[arg3]] VPD is not available.**

The vital product data (VPD) of the specified device is not available. VPD includes information such as the serial number and part number to uniquely identify the device.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information

Prefix: CMM **ID:** 0075

User Response

Complete the following steps until the problem is solved:

1. Reset the system-management processor in the node.
2. Replace the device.

- **0E010008 : Node [arg1] device [arg2][[arg3]] VPD is not available.**

The vital product data (VPD) of the specified device is not available. VPD includes information such as the serial number and part number to uniquely identify the device.

Severity

Warning

Serviceable

Yes

Automatically notify support

Yes

Alert Category

Nodes (Warning)

SNMP Trap ID

mmTrapBladeN

CIM Information

Prefix: CMM **ID:** 0075

User Response

Complete the following steps until the problem is solved:

1. Reset the system-management processor in the node.
2. Replace the device.

- **0E010009 : Node [arg1] device [arg2][[arg3]] VPD is not available.**

The vital product data (VPD) of the specified device is not available. VPD includes information such as the serial number and part number to uniquely identify the device.

Severity

Warning

Serviceable

Yes

Automatically notify support

Yes

Alert Category

Nodes (Warning)

SNMP Trap ID

mmTrapBladeN

CIM Information

Prefix: CMM **ID:** 0075

User Response

Complete the following steps until the problem is solved:

1. Reset the system-management processor in the node.
2. Replace the device.

- **0E01000A : Node [arg1] device [arg2][[arg3]] VPD is not available.**

  The vital product data (VPD) of the specified device is not available. VPD includes information such as the serial number and part number to uniquely identify the device.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0075

  User Response
  Complete the following steps until the problem is solved:

  1. Reset the system-management processor in the node.
  2. Replace the device.

- **0E01000B : Node [arg1] device [arg2][[arg3]] VPD is not available.**

  The vital product data (VPD) of the specified device is not available. VPD includes information such as the serial number and part number to uniquely identify the device.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0075

  User Response
  Complete the following steps until the problem is solved:

  1. Reset the system-management processor in the node.
  2. Replace the device.

- **0E01000C : Node [arg1] device [arg2][[arg3]] VPD is not available.**

  The vital product data (VPD) of the specified device is not available. VPD includes information such as the serial number and part number to uniquely identify the device.

  Severity
  Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0075

User Response
Complete the following steps until the problem is solved:

1. Reset the system-management processor in the node.
2. Replace the device.

- **0E01000D : Node [arg1] device [arg2][[arg3]] VPD is not available.**

The vital product data (VPD) of the specified device is not available. VPD includes information such as the serial number and part number to uniquely identify the device.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0075

User Response
Complete the following steps until the problem is solved:

1. Reset the system-management processor in the node.
2. Replace the device.

- **0E01000E : Node [arg1] device [arg2][[arg3]] VPD is not available.**

The vital product data (VPD) of the specified device is not available. VPD includes information such as the serial number and part number to uniquely identify the device.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category

Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0075

User Response
Complete the following steps until the problem is solved:

1. Reset the system-management processor in the node.
2. Replace the device.

- **0E020001 : The system-management processor on [arg1] was reset by the Chassis Management Module for system management bus service.**

  The Chassis Management Module has reset the system-management processor in the specified node one or more times for establishing communication with the system-management processor.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0747

  User Response
  Information only; no action is required.

- **0E020002 : The system-management processor on [arg1] was reset by the Chassis Management Module for system management bus service.**

  The Chassis Management Module has reset the system-management processor in the specified node one or more times for establishing communication with the system-management processor.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0747

User Response
Information only; no action is required.

- **0E020003 : The system-management processor on [arg1] was reset by the Chassis Management Module for system management bus service.**

  The Chassis Management Module has reset the system-management processor in the specified node one or more times for establishing communication with the system-management processor.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0747

  User Response
  Information only; no action is required.

- **0E020004 : The system-management processor on [arg1] was reset by the Chassis Management Module for system management bus service.**

  The Chassis Management Module has reset the system-management processor in the specified node one or more times for establishing communication with the system-management processor.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0747

  User Response
  Information only; no action is required.

- **0E020005 : The system-management processor on [arg1] was reset by the Chassis Management Module for system management bus service.**

  The Chassis Management Module has reset the system-management processor in the specified node one or more times for establishing communication with the system-management processor.

  Severity
  Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0747

User Response
Information only; no action is required.

- **0E020006 : The system-management processor on [arg1] was reset by the Chassis Management Module for system management bus service.**

  The Chassis Management Module has reset the system-management processor in the specified node one or more times for establishing communication with the system-management processor.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0747

  User Response
  Information only; no action is required.

- **0E020007 : The system-management processor on [arg1] was reset by the Chassis Management Module for system management bus service.**

  The Chassis Management Module has reset the system-management processor in the specified node one or more times for establishing communication with the system-management processor.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0747

User Response
Information only; no action is required.

- **0E020008 : The system-management processor on [arg1] was reset by the Chassis Management Module for system management bus service.**

  The Chassis Management Module has reset the system-management processor in the specified node one or more times for establishing communication with the system-management processor.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0747

  User Response
  Information only; no action is required.

- **0E020009 : The system-management processor on [arg1] was reset by the Chassis Management Module for system management bus service.**

  The Chassis Management Module has reset the system-management processor in the specified node one or more times for establishing communication with the system-management processor.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0747

  User Response
  Information only; no action is required.

- **0E02000A : The system-management processor on [arg1] was reset by the Chassis Management Module for system management bus service.**

  The Chassis Management Module has reset the system-management processor in the specified node one or more times for establishing communication with the system-management processor.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0747

User Response
Information only; no action is required.

- **0E02000B : The system-management processor on [arg1] was reset by the Chassis Management Module for system management bus service.**

  The Chassis Management Module has reset the system-management processor in the specified node one or more times for establishing communication with the system-management processor.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0747

  User Response
  Information only; no action is required.

- **0E02000C : The system-management processor on [arg1] was reset by the Chassis Management Module for system management bus service.**

  The Chassis Management Module has reset the system-management processor in the specified node one or more times for establishing communication with the system-management processor.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0747

User Response
Information only; no action is required.

- **0E02000D : The system-management processor on [arg1] was reset by the Chassis Management Module for system management bus service.**

  The Chassis Management Module has reset the system-management processor in the specified node one or more times for establishing communication with the system-management processor.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0747

  User Response
  Information only; no action is required.

- **0E02000E : The system-management processor on [arg1] was reset by the Chassis Management Module for system management bus service.**

  The Chassis Management Module has reset the system-management processor in the specified node one or more times for establishing communication with the system-management processor.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0747

  User Response
  Information only; no action is required.

- **0E200001 : Power denied to node [arg1] because it has unidentified hardware.**

The specified node contains components that the Chassis Management Module cannot identify. For example, the node might contain an expansion card that is not recognized. Therefore, the power requirements of the component cannot be determined.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0170

User Response
Complete the following steps until the problem is solved:

1. Check the Chassis Management Module event log for other problems pertaining to the node, such as invalid vital product data (VPD), and solve them.
2. If new hardware has been added to the node, check the firmware change history for applicable updates and, if necessary, update the node firmware.
3. Try running the node without optional components such as expansion cards.

- **0E200002 : Power denied to node [arg1] because it has unidentified hardware.**

The specified node contains components that the Chassis Management Module cannot identify. For example, the node might contain an expansion card that is not recognized. Therefore, the power requirements of the component cannot be determined.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0170

User Response
Complete the following steps until the problem is solved:

1. Check the Chassis Management Module event log for other problems pertaining to the node, such as invalid vital product data (VPD), and solve them.
2. If new hardware has been added to the node, check the firmware change history for applicable updates and, if necessary, update the node firmware.

3. Try running the node without optional components such as expansion cards.

- **0E200003 : Power denied to node [arg1] because it has unidentified hardware.**

  The specified node contains components that the Chassis Management Module cannot identify. For example, the node might contain an expansion card that is not recognized. Therefore, the power requirements of the component cannot be determined.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0170

  User Response
  Complete the following steps until the problem is solved:

  1. Check the Chassis Management Module event log for other problems pertaining to the node, such as invalid vital product data (VPD), and solve them.
  2. If new hardware has been added to the node, check the firmware change history for applicable updates and, if necessary, update the node firmware.
  3. Try running the node without optional components such as expansion cards.

- **0E200004 : Power denied to node [arg1] because it has unidentified hardware.**

  The specified node contains components that the Chassis Management Module cannot identify. For example, the node might contain an expansion card that is not recognized. Therefore, the power requirements of the component cannot be determined.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0170

  User Response
  Complete the following steps until the problem is solved:

  1. Check the Chassis Management Module event log for other problems pertaining to the node, such as invalid vital product data (VPD), and solve them.

2. If new hardware has been added to the node, check the firmware change history for applicable updates and, if necessary, update the node firmware.
3. Try running the node without optional components such as expansion cards.

- **0E200005 : Power denied to node [arg1] because it has unidentified hardware.**

  The specified node contains components that the Chassis Management Module cannot identify. For example, the node might contain an expansion card that is not recognized. Therefore, the power requirements of the component cannot be determined.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0170

  User Response
  Complete the following steps until the problem is solved:

  1. Check the Chassis Management Module event log for other problems pertaining to the node, such as invalid vital product data (VPD), and solve them.
  2. If new hardware has been added to the node, check the firmware change history for applicable updates and, if necessary, update the node firmware.
  3. Try running the node without optional components such as expansion cards.

- **0E200006 : Power denied to node [arg1] because it has unidentified hardware.**

  The specified node contains components that the Chassis Management Module cannot identify. For example, the node might contain an expansion card that is not recognized. Therefore, the power requirements of the component cannot be determined.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0170

  User Response
  Complete the following steps until the problem is solved:

1. Check the Chassis Management Module event log for other problems pertaining to the node, such as invalid vital product data (VPD), and solve them.
2. If new hardware has been added to the node, check the firmware change history for applicable updates and, if necessary, update the node firmware.
3. Try running the node without optional components such as expansion cards.

- **0E200007 : Power denied to node [arg1] because it has unidentified hardware.**

  The specified node contains components that the Chassis Management Module cannot identify. For example, the node might contain an expansion card that is not recognized. Therefore, the power requirements of the component cannot be determined.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0170

  User Response
  Complete the following steps until the problem is solved:

  1. Check the Chassis Management Module event log for other problems pertaining to the node, such as invalid vital product data (VPD), and solve them.
  2. If new hardware has been added to the node, check the firmware change history for applicable updates and, if necessary, update the node firmware.
  3. Try running the node without optional components such as expansion cards.

- **0E200008 : Power denied to node [arg1] because it has unidentified hardware.**

  The specified node contains components that the Chassis Management Module cannot identify. For example, the node might contain an expansion card that is not recognized. Therefore, the power requirements of the component cannot be determined.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0170

User Response

Complete the following steps until the problem is solved:

1. Check the Chassis Management Module event log for other problems pertaining to the node, such as invalid vital product data (VPD), and solve them.
2. If new hardware has been added to the node, check the firmware change history for applicable updates and, if necessary, update the node firmware.
3. Try running the node without optional components such as expansion cards.

- **0E200009 : Power denied to node [arg1] because it has unidentified hardware.**

The specified node contains components that the Chassis Management Module cannot identify. For example, the node might contain an expansion card that is not recognized. Therefore, the power requirements of the component cannot be determined.

Severity

Warning

Serviceable

Yes

Automatically notify support

No

Alert Category

Nodes (Warning)

SNMP Trap ID

mmTrapBladeN

CIM Information

Prefix: CMM **ID:** 0170

User Response

Complete the following steps until the problem is solved:

1. Check the Chassis Management Module event log for other problems pertaining to the node, such as invalid vital product data (VPD), and solve them.
2. If new hardware has been added to the node, check the firmware change history for applicable updates and, if necessary, update the node firmware.
3. Try running the node without optional components such as expansion cards.

- **0E20000A : Power denied to node [arg1] because it has unidentified hardware.**

The specified node contains components that the Chassis Management Module cannot identify. For example, the node might contain an expansion card that is not recognized. Therefore, the power requirements of the component cannot be determined.

Severity

Warning

Serviceable

Yes

Automatically notify support

No

Alert Category

Nodes (Warning)

SNMP Trap ID

mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0170

User Response
Complete the following steps until the problem is solved:

1. Check the Chassis Management Module event log for other problems pertaining to the node, such as invalid vital product data (VPD), and solve them.
2. If new hardware has been added to the node, check the firmware change history for applicable updates and, if necessary, update the node firmware.
3. Try running the node without optional components such as expansion cards.

- **0E20000B : Power denied to node [arg1] because it has unidentified hardware.**

The specified node contains components that the Chassis Management Module cannot identify. For example, the node might contain an expansion card that is not recognized. Therefore, the power requirements of the component cannot be determined.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0170

User Response
Complete the following steps until the problem is solved:

1. Check the Chassis Management Module event log for other problems pertaining to the node, such as invalid vital product data (VPD), and solve them.
2. If new hardware has been added to the node, check the firmware change history for applicable updates and, if necessary, update the node firmware.
3. Try running the node without optional components such as expansion cards.

- **0E20000C : Power denied to node [arg1] because it has unidentified hardware.**

The specified node contains components that the Chassis Management Module cannot identify. For example, the node might contain an expansion card that is not recognized. Therefore, the power requirements of the component cannot be determined.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0170

User Response
Complete the following steps until the problem is solved:

1. Check the Chassis Management Module event log for other problems pertaining to the node, such as invalid vital product data (VPD), and solve them.
2. If new hardware has been added to the node, check the firmware change history for applicable updates and, if necessary, update the node firmware.
3. Try running the node without optional components such as expansion cards.

- **0E20000D : Power denied to node [arg1] because it has unidentified hardware.**

The specified node contains components that the Chassis Management Module cannot identify. For example, the node might contain an expansion card that is not recognized. Therefore, the power requirements of the component cannot be determined.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0170

User Response
Complete the following steps until the problem is solved:

1. Check the Chassis Management Module event log for other problems pertaining to the node, such as invalid vital product data (VPD), and solve them.
2. If new hardware has been added to the node, check the firmware change history for applicable updates and, if necessary, update the node firmware.
3. Try running the node without optional components such as expansion cards.

- **0E20000E : Power denied to node [arg1] because it has unidentified hardware.**

The specified node contains components that the Chassis Management Module cannot identify. For example, the node might contain an expansion card that is not recognized. Therefore, the power requirements of the component cannot be determined.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0170

User Response
Complete the following steps until the problem is solved:

1. Check the Chassis Management Module event log for other problems pertaining to the node, such as invalid vital product data (VPD), and solve them.
2. If new hardware has been added to the node, check the firmware change history for applicable updates and, if necessary, update the node firmware.
3. Try running the node without optional components such as expansion cards.

- **0EA00001 : I/O module [arg1] fault.**

  A fault has occurred in the specified I/O module. This event is a general fault alert. A more specific event related to a current fault might be reported in the Chassis Management Module event log.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  I/O Modules (Critical)

  SNMP Trap ID
  mmTrapIOC

  CIM Information
  Prefix: CMM **ID:** 0051

  User Response
  Replace the I/O module.

- **0EA00002 : I/O module [arg1] fault.**

  A fault has occurred in the specified I/O module. This event is a general fault alert. A more specific event related to a current fault might be reported in the Chassis Management Module event log.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  I/O Modules (Critical)

  SNMP Trap ID
  mmTrapIOC

  CIM Information

Prefix: CMM **ID:** 0051

User Response
Replace the I/O module.

- **0EA00003 : I/O module [arg1] fault.**

  A fault has occurred in the specified I/O module. This event is a general fault alert. A more specific event related to a current fault might be reported in the Chassis Management Module event log.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  I/O Modules (Critical)

  SNMP Trap ID
  mmTrapIOC

  CIM Information
  Prefix: CMM **ID:** 0051

  User Response
  Replace the I/O module.

- **0EA00004 : I/O module [arg1] fault.**

  A fault has occurred in the specified I/O module. This event is a general fault alert. A more specific event related to a current fault might be reported in the Chassis Management Module event log.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  I/O Modules (Critical)

  SNMP Trap ID
  mmTrapIOC

  CIM Information
  Prefix: CMM **ID:** 0051

  User Response
  Replace the I/O module.

- **0EA01001 : VPD for I/O Module [arg1] is not available.**

  The Chassis Management Module is not able to read the vital product data (VPD) for the specific I/O module.

  Severity
  Error

  Serviceable

Yes

Automatically notify support
No

Alert Category
I/O Modules (Critical)

SNMP Trap ID
mmTrapIOC

CIM Information
Prefix: CMM **ID:** 0240

User Response
Complete the following steps until the problem is solved:

1. Perform a service-level reset of the I/O module. Note that this might affect network services.
2. Replace the I/O module.

- **0EA01002 : VPD for I/O Module [arg1] is not available.**

The Chassis Management Module is not able to read the vital product data (VPD) for the specific I/O module.

Severity
Error

Serviceable
Yes

Automatically notify support
No

Alert Category
I/O Modules (Critical)

SNMP Trap ID
mmTrapIOC

CIM Information
Prefix: CMM **ID:** 0240

User Response
Complete the following steps until the problem is solved:

1. Perform a service-level reset of the I/O module. Note that this might affect network services.
2. Replace the I/O module.

- **0EA01003 : VPD for I/O Module [arg1] is not available.**

The Chassis Management Module is not able to read the vital product data (VPD) for the specific I/O module.

Severity
Error

Serviceable
Yes

Automatically notify support
No

Alert Category
I/O Modules (Critical)

SNMP Trap ID
mmTrapIOC

CIM Information
Prefix: CMM **ID:** 0240

User Response
Complete the following steps until the problem is solved:

1. Perform a service-level reset of the I/O module. Note that this might affect network services.
2. Replace the I/O module.

- **0EA01004 : VPD for I/O Module [arg1] is not available.**

The Chassis Management Module is not able to read the vital product data (VPD) for the specific I/O module.

Severity
Error

Serviceable
Yes

Automatically notify support
No

Alert Category
I/O Modules (Critical)

SNMP Trap ID
mmTrapIOC

CIM Information
Prefix: CMM **ID:** 0240

User Response
Complete the following steps until the problem is solved:

1. Perform a service-level reset of the I/O module. Note that this might affect network services.
2. Replace the I/O module.

- **0EA02001 : Hardware inserted in [arg1].**

Hardware has been installed in the specified bay in the chassis.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0100

User Response
Information only; no action is required.

- **0EA02002 : Hardware inserted in [arg1].**

  Hardware has been installed in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0100

  User Response
  Information only; no action is required.
- **0EA02003 : Hardware inserted in [arg1].**

  Hardware has been installed in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0100

  User Response
  Information only; no action is required.
- **0EA02004 : Hardware inserted in [arg1].**

  Hardware has been installed in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0100

User Response
Information only; no action is required.

- **0EA02101 : Discovered device [arg1] in [arg2], CRC: [arg3].**

  Hardware has been discovered successfully in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0102

  User Response
  Information only; no action is required.

- **0EA02102 : Discovered device [arg1] in [arg2], CRC: [arg3].**

  Hardware has been discovered successfully in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0102

  User Response
  Information only; no action is required.

- **0EA02103 : Discovered device [arg1] in [arg2], CRC: [arg3].**

  Hardware has been discovered successfully in the specified bay in the chassis.

  Severity
  Informational

  Serviceable

No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0102

User Response
Information only; no action is required.

- **0EA02104 : Discovered device [arg1] in [arg2], CRC: [arg3].**

Hardware has been discovered successfully in the specified bay in the chassis.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0102

User Response
Information only; no action is required.

- **0EA03101 : Failed to discover device [arg1] in [arg2].**

Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0103

User Response

Information only; no action is required.

- **0EA03102 : Failed to discover device [arg1] in [arg2].**

  Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0103

  User Response
  Information only; no action is required.

- **0EA03103 : Failed to discover device [arg1] in [arg2].**

  Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0103

  User Response
  Information only; no action is required.

- **0EA03104 : Failed to discover device [arg1] in [arg2].**

  Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support

No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0103

User Response
Information only; no action is required.

- **0EA04001 : Hardware removed from [arg1].**

  Hardware has been removed from the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0101

  User Response
  Information only; no action is required.

- **0EA04002 : Hardware removed from [arg1].**

  Hardware has been removed from the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0101

  User Response
  Information only; no action is required.

- **0EA04003 : Hardware removed from [arg1].**

  Hardware has been removed from the specified bay in the chassis.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0101

User Response
Information only; no action is required.

- **0EA04004 : Hardware removed from [arg1].**

  Hardware has been removed from the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0101

  User Response
  Information only; no action is required.

- **0EA06001 : I/O module [arg1] was instructed to power off by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified I/O module has been powered off by the specified user.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0689

User Response
Information only; no action is required.

- **0EA06002 : I/O module [arg1] was instructed to power off by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified I/O module has been powered off by the specified user.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0689

  User Response
  Information only; no action is required.

- **0EA06003 : I/O module [arg1] was instructed to power off by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified I/O module has been powered off by the specified user.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0689

  User Response
  Information only; no action is required.

- **0EA06004 : I/O module [arg1] was instructed to power off by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified I/O module has been powered off by the specified user.

  Severity
  Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0689

User Response
Information only; no action is required.

- **0EA08001 : I/O module [arg1] was instructed to power on by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified I/O module has been powered on by the specified user.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0688

  User Response
  Information only; no action is required.

- **0EA08002 : I/O module [arg1] was instructed to power on by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified I/O module has been powered on by the specified user.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0688

User Response
Information only; no action is required.

- **0EA08003 : I/O module [arg1] was instructed to power on by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified I/O module has been powered on by the specified user.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0688

  User Response
  Information only; no action is required.

- **0EA08004 : I/O module [arg1] was instructed to power on by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified I/O module has been powered on by the specified user.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0688

  User Response
  Information only; no action is required.

- **0EA09001 : The network port on I/O module [arg1] has been disabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has disabled the external ports in the specified I/O module.

  Severity
  Informational

  Serviceable
  No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0659

User Response
Information only; no action is required.

- **0EA09002 : The network port on I/O module [arg1] has been disabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has disabled the external ports in the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0659

  User Response
  Information only; no action is required.

- **0EA09003 : The network port on I/O module [arg1] has been disabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has disabled the external ports in the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0659

  User Response
  Information only; no action is required.

- **0EA09004 : The network port on I/O module [arg1] has been disabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has disabled the external ports in the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0659

  User Response
  Information only; no action is required.
- **0EA09101 : The network port on I/O module [arg1] has been enabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has enabled the external ports in the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0658

  User Response
  Information only; no action is required.
- **0EA09102 : The network port on I/O module [arg1] has been enabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has enabled the external ports in the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0658

User Response
Information only; no action is required.

- **0EA09103 : The network port on I/O module [arg1] has been enabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has enabled the external ports in the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0658

  User Response
  Information only; no action is required.

- **0EA09104 : The network port on I/O module [arg1] has been enabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has enabled the external ports in the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0658

  User Response
  Information only; no action is required.

- **0EA0A001 : I/O module [arg1] IP address was changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

The specified user has changed the IP address of the specified I/O module.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0669

User Response
Information only; no action is required.

- **0EA0A002 : I/O module [arg1] IP address was changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IP address of the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0669

  User Response
  Information only; no action is required.

- **0EA0A003 : I/O module [arg1] IP address was changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IP address of the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0669

User Response
Information only; no action is required.

- **0EA0A004 : I/O module [arg1] IP address was changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IP address of the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0669

  User Response
  Information only; no action is required.

- **0EA0C001 : I/O module [arg1] is incompatible with the node configuration.**

  The I/O fabric type of the expansion card in the node is not compatible with the specified I/O module.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  I/O Modules (Warning)

  SNMP Trap ID
  mmTrapION

  CIM Information
  Prefix: CMM **ID:** 0061

  User Response
  Make sure that the expansion card in the node and the I/O module are compatible (are of the same I/O fabric type).

- **0EA0C002 : I/O module [arg1] is incompatible with the node configuration.**

  The I/O fabric type of the expansion card in the node is not compatible with the specified I/O module.

  Severity

Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
I/O Modules (Warning)

SNMP Trap ID
mmTrapION

CIM Information
Prefix: CMM **ID:** 0061

User Response
Make sure that the expansion card in the node and the I/O module are compatible (are of the same I/O fabric type).

- **0EA0C003 : I/O module [arg1] is incompatible with the node configuration.**

  The I/O fabric type of the expansion card in the node is not compatible with the specified I/O module.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  I/O Modules (Warning)

  SNMP Trap ID
  mmTrapION

  CIM Information
  Prefix: CMM **ID:** 0061

  User Response
  Make sure that the expansion card in the node and the I/O module are compatible (are of the same I/O fabric type).

- **0EA0C004 : I/O module [arg1] is incompatible with the node configuration.**

  The I/O fabric type of the expansion card in the node is not compatible with the specified I/O module.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  I/O Modules (Warning)

  SNMP Trap ID
  mmTrapION

CIM Information
Prefix: CMM **ID:** 0061

User Response
Make sure that the expansion card in the node and the I/O module are compatible (are of the same I/O fabric type).

- **0EA0D001 : I/O module [arg1] POST timeout.**

The specified I/O module is taking too long to complete the power-on self-test (POST).

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
I/O Modules (Warning)

SNMP Trap ID
mmTrapION

CIM Information
Prefix: CMM **ID:** 0063

User Response
The I/O module might still be in the process of starting. Therefore, if no recovery message is displayed within 15 minutes, complete the following steps until the problem is solved:

1. Attempt to restart the I/O module, and specify the extended POST process to receive a more specific error code.
2. Perform a service-level reset of the I/O module, which restarts the I/O module.
3. Reinstall the same level of firmware.
4. Replace the I/O module.

- **0EA0D002 : I/O module [arg1] POST timeout.**

The specified I/O module is taking too long to complete the power-on self-test (POST).

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
I/O Modules (Warning)

SNMP Trap ID
mmTrapION

CIM Information
Prefix: CMM **ID:** 0063

User Response
The I/O module might still be in the process of starting. Therefore, if no recovery message is displayed within 15 minutes, complete the following steps until the problem is solved:

1. Attempt to restart the I/O module, and specify the extended POST process to receive a more specific error code.
2. Perform a service-level reset of the I/O module, which restarts the I/O module.
3. Reinstall the same level of firmware.
4. Replace the I/O module.

- **0EA0D003 : I/O module [arg1] POST timeout.**

  The specified I/O module is taking too long to complete the power-on self-test (POST).

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  I/O Modules (Warning)

  SNMP Trap ID
  mmTrapION

  CIM Information
  Prefix: CMM **ID:** 0063

  User Response
  The I/O module might still be in the process of starting. Therefore, if no recovery message is displayed within 15 minutes, complete the following steps until the problem is solved:

  1. Attempt to restart the I/O module, and specify the extended POST process to receive a more specific error code.
  2. Perform a service-level reset of the I/O module, which restarts the I/O module.
  3. Reinstall the same level of firmware.
  4. Replace the I/O module.

- **0EA0D004 : I/O module [arg1] POST timeout.**

  The specified I/O module is taking too long to complete the power-on self-test (POST).

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  I/O Modules (Warning)

  SNMP Trap ID
  mmTrapION

  CIM Information
  Prefix: CMM **ID:** 0063

  User Response

The I/O module might still be in the process of starting. Therefore, if no recovery message is displayed within 15 minutes, complete the following steps until the problem is solved:

1. Attempt to restart the I/O module, and specify the extended POST process to receive a more specific error code.
2. Perform a service-level reset of the I/O module, which restarts the I/O module.
3. Reinstall the same level of firmware.
4. Replace the I/O module.

- **0EA0D501 : Attempt to set port speed/mode on I/O Module [arg1] by user [arg2].**

  A user has attempted to set the port speed and mode on the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0749

  User Response
  No actions taken.

- **0EA0D502 : Attempt to set port speed/mode on I/O Module [arg1] by user [arg2].**

  A user has attempted to set the port speed and mode on the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0749

  User Response
  No actions taken.

- **0EA0D503 : Attempt to set port speed/mode on I/O Module [arg1] by user [arg2].**

  A user has attempted to set the port speed and mode on the specified I/O module.

  Severity
  Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0749

User Response
No actions taken.

- **0EA0D504 : Attempt to set port speed/mode on I/O Module [arg1] by user [arg2].**

  A user has attempted to set the port speed and mode on the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0749

  User Response
  No actions taken.

- **0EA0D601 : Port speed/mode is changed on I/O Module [arg1] by user [arg2].**

  The port speed and mode has been changed on the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0750

  User Response

Information only; no action is required.

- **0EA0D602 : Port speed/mode is changed on I/O Module [arg1] by user [arg2].**

  The port speed and mode has been changed on the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0750

  User Response
  Information only; no action is required.

- **0EA0D603 : Port speed/mode is changed on I/O Module [arg1] by user [arg2].**

  The port speed and mode has been changed on the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0750

  User Response
  Information only; no action is required.

- **0EA0D604 : Port speed/mode is changed on I/O Module [arg1] by user [arg2].**

  The port speed and mode has been changed on the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0750

User Response
Information only; no action is required.

- **0EA0D801 : I/O module [arg1] firmware image [arg2] activated by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has activated the firmware image.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0778

  User Response
  Information only; no action is required.

- **0EA0D802 : I/O module [arg1] firmware image [arg2] activated by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has activated the firmware image.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0778

  User Response
  Information only; no action is required.

- **0EA0D803 : I/O module [arg1] firmware image [arg2] activated by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has activated the firmware image.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0778

User Response
Information only; no action is required.

- **0EA0D804 : I/O module [arg1] firmware image [arg2] activated by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has activated the firmware image.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0778

  User Response
  Information only; no action is required.

- **0EA0D901 : I/O module [arg1] firmware image [arg2] failed to activate by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has failed to activate the firmware image.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0779

User Response
Retry the I/O Module firmware activation a few minutes after the intial failure. If the activation fails again, reset the I/O Module and try the I/O Module firmware activation again. If the activation fails again, please contact Support.

- **0EA0D902 : I/O module [arg1] firmware image [arg2] failed to activate by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has failed to activate the firmware image.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0779

  User Response
  Retry the I/O Module firmware activation a few minutes after the intial failure. If the activation fails again, reset the I/O Module and try the I/O Module firmware activation again. If the activation fails again, please contact Support.

- **0EA0D903 : I/O module [arg1] firmware image [arg2] failed to activate by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has failed to activate the firmware image.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0779

  User Response
  Retry the I/O Module firmware activation a few minutes after the intial failure. If the activation fails again, reset the I/O Module and try the I/O Module firmware activation again. If the activation fails again, please contact Support.

- **0EA0D904 : I/O module [arg1] firmware image [arg2] failed to activate by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has failed to activate the firmware image.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0779

  User Response
  Retry the I/O Module firmware activation a few minutes after the intial failure. If the activation fails again, reset the I/O Module and try the I/O Module firmware activation again. If the activation fails again, please contact Support.
- **0EA0DB01 : Duplicate route detected to I/O module [arg1].**

  The Chassis Management Module has detected a duplicate route to the specified I/O module because the internal and external management IP addresses are the same. The CMM will ignore the internal route.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0245

  User Response
  Information only; no action is required.
- **0EA0DB02 : Duplicate route detected to I/O module [arg1].**

  The Chassis Management Module has detected a duplicate route to the specified I/O module because the internal and external management IP addresses are the same. The CMM will ignore the internal route.

  Severity
  Informational

  Serviceable
  No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0245

User Response
Information only; no action is required.

- **0EA0DB03 : Duplicate route detected to I/O module [arg1].**

  The Chassis Management Module has detected a duplicate route to the specified I/O module because the internal and external management IP addresses are the same. The CMM will ignore the internal route.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0245

  User Response
  Information only; no action is required.

- **0EA0DB04 : Duplicate route detected to I/O module [arg1].**

  The Chassis Management Module has detected a duplicate route to the specified I/O module because the internal and external management IP addresses are the same. The CMM will ignore the internal route.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0245

  User Response
  Information only; no action is required.

- **0EA0E001 : I/O module [arg1] POST failure, POST status: [arg2].**

  An error has occurred in the specified I/O module during the power-on self-test (POST). If the error is not critical, the I/O module might continue to start and function normally. If the error is critical, the I/O module will not start, and the fault LED on the I/O module will be lit.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  I/O Modules (Critical)

  SNMP Trap ID
  mmTrapIOC

  CIM Information
  Prefix: CMM **ID:** 0065

  User Response
  Complete the following steps until the problem is solved:

  1. See the documentation for the specified I/O module for information about the meaning of the POST status and recovery actions that you should take.
  2. Temporarily disable all communication between the nodes and the specified I/O module in the chassis to reduce interruptions to the services that the nodes provide.
  3. Perform a service-level reset of the I/O module, which restarts the I/O module.
  4. If the firmware in the I/O module was recently updated and the POST error is not critical, revert to the previous level of firmware.
  5. Replace the I/O module.

- **0EA0E002 : I/O module [arg1] POST failure, POST status: [arg2].**

  An error has occurred in the specified I/O module during the power-on self-test (POST). If the error is not critical, the I/O module might continue to start and function normally. If the error is critical, the I/O module will not start, and the fault LED on the I/O module will be lit.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  I/O Modules (Critical)

  SNMP Trap ID
  mmTrapIOC

  CIM Information
  Prefix: CMM **ID:** 0065

  User Response
  Complete the following steps until the problem is solved:

1. See the documentation for the specified I/O module for information about the meaning of the POST status and recovery actions that you should take.
2. Temporarily disable all communication between the nodes and the specified I/O module in the chassis to reduce interruptions to the services that the nodes provide.
3. Perform a service-level reset of the I/O module, which restarts the I/O module.
4. If the firmware in the I/O module was recently updated and the POST error is not critical, revert to the previous level of firmware.
5. Replace the I/O module.

- **0EA0E003 : I/O module [arg1] POST failure, POST status: [arg2].**

  An error has occurred in the specified I/O module during the power-on self-test (POST). If the error is not critical, the I/O module might continue to start and function normally. If the error is critical, the I/O module will not start, and the fault LED on the I/O module will be lit.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  I/O Modules (Critical)

  SNMP Trap ID
  mmTrapIOC

  CIM Information
  Prefix: CMM **ID:** 0065

  User Response
  Complete the following steps until the problem is solved:

  1. See the documentation for the specified I/O module for information about the meaning of the POST status and recovery actions that you should take.
  2. Temporarily disable all communication between the nodes and the specified I/O module in the chassis to reduce interruptions to the services that the nodes provide.
  3. Perform a service-level reset of the I/O module, which restarts the I/O module.
  4. If the firmware in the I/O module was recently updated and the POST error is not critical, revert to the previous level of firmware.
  5. Replace the I/O module.

- **0EA0E004 : I/O module [arg1] POST failure, POST status: [arg2].**

  An error has occurred in the specified I/O module during the power-on self-test (POST). If the error is not critical, the I/O module might continue to start and function normally. If the error is critical, the I/O module will not start, and the fault LED on the I/O module will be lit.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

Alert Category
I/O Modules (Critical)

SNMP Trap ID
mmTrapIOC

CIM Information
Prefix: CMM **ID:** 0065

User Response
Complete the following steps until the problem is solved:

1. See the documentation for the specified I/O module for information about the meaning of the POST status and recovery actions that you should take.
2. Temporarily disable all communication between the nodes and the specified I/O module in the chassis to reduce interruptions to the services that the nodes provide.
3. Perform a service-level reset of the I/O module, which restarts the I/O module.
4. If the firmware in the I/O module was recently updated and the POST error is not critical, revert to the previous level of firmware.
5. Replace the I/O module.

- **0EA0ED01 : I/O module [arg1] unrecognized.**

  The Chassis Management Module does not recognize specified I/O-module type.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  I/O Modules (Warning)

  SNMP Trap ID
  mmTrapION

  CIM Information
  Prefix: CMM **ID:** 0248

  User Response
  Check the ServerProven list to make sure that the chassis supports the I/O module. Update to CMM firmware to a version that supports the I/O module.

- **0EA0ED02 : I/O module [arg1] unrecognized.**

  The Chassis Management Module does not recognize specified I/O-module type.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  I/O Modules (Warning)

SNMP Trap ID
mmTrapION

CIM Information
Prefix: CMM **ID:** 0248

User Response
Check the ServerProven list to make sure that the chassis supports the I/O module. Update to CMM firmware to a version that supports the I/O module.

- **0EA0ED03 : I/O module [arg1] unrecognized.**

The Chassis Management Module does not recognize specified I/O-module type.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
I/O Modules (Warning)

SNMP Trap ID
mmTrapION

CIM Information
Prefix: CMM **ID:** 0248

User Response
Check the ServerProven list to make sure that the chassis supports the I/O module. Update to CMM firmware to a version that supports the I/O module.

- **0EA0ED04 : I/O module [arg1] unrecognized.**

The Chassis Management Module does not recognize specified I/O-module type.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
I/O Modules (Warning)

SNMP Trap ID
mmTrapION

CIM Information
Prefix: CMM **ID:** 0248

User Response
Check the ServerProven list to make sure that the chassis supports the I/O module. Update to CMM firmware to a version that supports the I/O module.

- **0EA0F101 : I/O module [arg1] enabled Protected Mode control of IP configuration.**

I/O module specified enabled Protected Mode control of IP configuration.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0426

User Response
Information only; no action is required.

- **0EA0F102 : I/O module [arg1] enabled Protected Mode control of IP configuration.**

  I/O module specified enabled Protected Mode control of IP configuration.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0426

  User Response
  Information only; no action is required.

- **0EA0F103 : I/O module [arg1] enabled Protected Mode control of IP configuration.**

  I/O module specified enabled Protected Mode control of IP configuration.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information

Prefix: CMM **ID:** 0426

User Response
Information only; no action is required.

- **0EA0F104 : I/O module [arg1] enabled Protected Mode control of IP configuration.**

  I/O module specified enabled Protected Mode control of IP configuration.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0426

  User Response
  Information only; no action is required.

- **0EA0F201 : I/O module [arg1] enabled Protected Mode control of external ports.**

  I/O module specified enabled Protected Mode control of external ports.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0427

  User Response
  Information only; no action is required.

- **0EA0F202 : I/O module [arg1] enabled Protected Mode control of external ports.**

  I/O module specified enabled Protected Mode control of external ports.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0427

User Response
Information only; no action is required.

- **0EA0F203 : I/O module [arg1] enabled Protected Mode control of external ports.**

  I/O module specified enabled Protected Mode control of external ports.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0427

  User Response
  Information only; no action is required.

- **0EA0F204 : I/O module [arg1] enabled Protected Mode control of external ports.**

  I/O module specified enabled Protected Mode control of external ports.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0427

  User Response
  Information only; no action is required.

- **0EA0F301 : I/O module [arg1] enabled Protected Mode control of external management.**

  I/O module specified enabled Protected Mode control of external management.

  Severity

Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0428

User Response
Information only; no action is required.

- **0EA0F302 : I/O module [arg1] enabled Protected Mode control of external management.**

  I/O module specified enabled Protected Mode control of external management.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0428

  User Response
  Information only; no action is required.

- **0EA0F303 : I/O module [arg1] enabled Protected Mode control of external management.**

  I/O module specified enabled Protected Mode control of external management.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0428

User Response
Information only; no action is required.

- **0EA0F304 : I/O module [arg1] enabled Protected Mode control of external management.**

  I/O module specified enabled Protected Mode control of external management.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0428

  User Response
  Information only; no action is required.

- **0EA0F401 : I/O module [arg1] enabled Protected Mode control of reset configuration to defaults.**

  I/O module specified enabled Protected Mode control of reset configuration to defaults.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0429

  User Response
  Information only; no action is required.

- **0EA0F402 : I/O module [arg1] enabled Protected Mode control of reset configuration to defaults.**

  I/O module specified enabled Protected Mode control of reset configuration to defaults.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category

I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0429

User Response
Information only; no action is required.

- **0EA0F403 : I/O module [arg1] enabled Protected Mode control of reset configuration to defaults.**

  I/O module specified enabled Protected Mode control of reset configuration to defaults.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0429

  User Response
  Information only; no action is required.

- **0EA0F404 : I/O module [arg1] enabled Protected Mode control of reset configuration to defaults.**

  I/O module specified enabled Protected Mode control of reset configuration to defaults.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0429

  User Response
  Information only; no action is required.

- **0EA0F501 : I/O module [arg1] is in Protected Mode without permission from the CMM.**

  I/O module specified is in Protected Mode without CMM's permission.

  Severity
  Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0430

User Response
Information only; no action is required.

- **0EA0F502 : I/O module [arg1] is in Protected Mode without permission from the CMM.**

I/O module specified is in Protected Mode without CMM's permission.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0430

User Response
Information only; no action is required.

- **0EA0F503 : I/O module [arg1] is in Protected Mode without permission from the CMM.**

I/O module specified is in Protected Mode without CMM's permission.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0430

User Response

Information only; no action is required.

- **0EA0F504 : I/O module [arg1] is in Protected Mode without permission from the CMM.**

  I/O module specified is in Protected Mode without CMM's permission.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0430

  User Response
  Information only; no action is required.

- **0EA0F601 : I/O module [arg1] Protected Mode permission and CMM configured permission are mismatched.**

  I/O module specified Protected Mode permission and CMM configured permission are mismatched.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0431

  User Response
  Information only; no action is required.

- **0EA0F602 : I/O module [arg1] Protected Mode permission and CMM configured permission are mismatched.**

  I/O module specified Protected Mode permission and CMM configured permission are mismatched.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0431

User Response
Information only; no action is required.

- **0EA0F603 : I/O module [arg1] Protected Mode permission and CMM configured permission are mismatched.**

  I/O module specified Protected Mode permission and CMM configured permission are mismatched.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0431

  User Response
  Information only; no action is required.

- **0EA0F604 : I/O module [arg1] Protected Mode permission and CMM configured permission are mismatched.**

  I/O module specified Protected Mode permission and CMM configured permission are mismatched.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0431

  User Response
  Information only; no action is required.

- **0EA0FE01 : I/O module [arg1] enabled Stacking Mode.**

  I/O module specified enabled Stacking Mode.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0432

User Response
Information only; no action is required.

- **0EA0FE02 : I/O module [arg1] enabled Stacking Mode.**

  I/O module specified enabled Stacking Mode.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0432

  User Response
  Information only; no action is required.

- **0EA0FE03 : I/O module [arg1] enabled Stacking Mode.**

  I/O module specified enabled Stacking Mode.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information

Prefix: CMM **ID:** 0432

User Response
Information only; no action is required.

- **0EA0FE04 : I/O module [arg1] enabled Stacking Mode.**

  I/O module specified enabled Stacking Mode.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0432

  User Response
  Information only; no action is required.

- **0EA12001 : I/O module [arg1] setting to preserve new IP configuration on all resets is enabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has enabled the setting to preserve new IP configuration on all resets in the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0660

  User Response
  Information only; no action is required.

- **0EA12002 : I/O module [arg1] setting to preserve new IP configuration on all resets is enabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has enabled the setting to preserve new IP configuration on all resets in the specified I/O module.

  Severity
  Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0660

User Response
Information only; no action is required.

- **0EA12003 : I/O module [arg1] setting to preserve new IP configuration on all resets is enabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has enabled the setting to preserve new IP configuration on all resets in the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0660

  User Response
  Information only; no action is required.

- **0EA12004 : I/O module [arg1] setting to preserve new IP configuration on all resets is enabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has enabled the setting to preserve new IP configuration on all resets in the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0660

User Response
Information only; no action is required.

- **0EA13001 : I/O module [arg1] setting to preserve new IP configuration on all resets is disabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has disabled the setting to preserve new IP configuration on all resets in the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0661

  User Response
  Information only; no action is required.

- **0EA13002 : I/O module [arg1] setting to preserve new IP configuration on all resets is disabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has disabled the setting to preserve new IP configuration on all resets in the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0661

  User Response
  Information only; no action is required.

- **0EA13003 : I/O module [arg1] setting to preserve new IP configuration on all resets is disabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has disabled the setting to preserve new IP configuration on all resets in the specified I/O module.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0661

User Response
Information only; no action is required.

- **0EA13004 : I/O module [arg1] setting to preserve new IP configuration on all resets is disabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has disabled the setting to preserve new IP configuration on all resets in the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0661

  User Response
  Information only; no action is required.

- **0EA14001 : I/O module [arg1] external management is enabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has modified the I/O module to enable external management.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID

mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0685

User Response
Information only; no action is required.

- **0EA14002 : I/O module [arg1] external management is enabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has modified the I/O module to enable external management.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0685

  User Response
  Information only; no action is required.

- **0EA14003 : I/O module [arg1] external management is enabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has modified the I/O module to enable external management.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0685

  User Response
  Information only; no action is required.

- **0EA14004 : I/O module [arg1] external management is enabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has modified the I/O module to enable external management.

  Severity

Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0685

User Response
Information only; no action is required.

- **0EA15001 : I/O module [arg1] IP subnet mask was changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IP subnet mask of the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0670

  User Response
  Information only; no action is required.

- **0EA15002 : I/O module [arg1] IP subnet mask was changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IP subnet mask of the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0670

User Response
Information only; no action is required.

- **0EA15003 : I/O module [arg1] IP subnet mask was changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IP subnet mask of the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0670

  User Response
  Information only; no action is required.

- **0EA15004 : I/O module [arg1] IP subnet mask was changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IP subnet mask of the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0670

  User Response
  Information only; no action is required.

- **0EA17001 : I/O module [arg1] IP gateway was changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IP gateway of the specified I/O module.

  Severity
  Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0671

User Response
Information only; no action is required.

- **0EA17002 : I/O module [arg1] IP gateway was changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IP gateway of the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0671

  User Response
  Information only; no action is required.

- **0EA17003 : I/O module [arg1] IP gateway was changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IP gateway of the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0671

User Response
Information only; no action is required.

- **0EA17004 : I/O module [arg1] IP gateway was changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IP gateway of the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0671

  User Response
  Information only; no action is required.

- **0EA18001 : I/O module [arg1] IP configuration method was changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IP configuration method of the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0672

  User Response
  Information only; no action is required.

- **0EA18002 : I/O module [arg1] IP configuration method was changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IP configuration method of the specified I/O module.

  Severity
  Informational

  Serviceable
  No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0672

User Response
Information only; no action is required.

- **0EA18003 : I/O module [arg1] IP configuration method was changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IP configuration method of the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0672

  User Response
  Information only; no action is required.

- **0EA18004 : I/O module [arg1] IP configuration method was changed to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IP configuration method of the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0672

  User Response
  Information only; no action is required.

- **0EA19001 : I/O module [arg1] IP DHCP address was changed to [arg2].**

  The IP DHCP address of the specified I/O module has been changed.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0673

  User Response
  Information only; no action is required.
- **0EA19002 : I/O module [arg1] IP DHCP address was changed to [arg2].**

  The IP DHCP address of the specified I/O module has been changed.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0673

  User Response
  Information only; no action is required.
- **0EA19003 : I/O module [arg1] IP DHCP address was changed to [arg2].**

  The IP DHCP address of the specified I/O module has been changed.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0673

User Response
Information only; no action is required.

- **0EA19004 : I/O module [arg1] IP DHCP address was changed to [arg2].**

  The IP DHCP address of the specified I/O module has been changed.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0673

  User Response
  Information only; no action is required.

- **0EA1A001 : I/O module [arg1] IP address was changed to [arg2] by the I/O module.**

  The IP address of the specified I/O module has been changed by the I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0674

  User Response
  Information only; no action is required.

- **0EA1A002 : I/O module [arg1] IP address was changed to [arg2] by the I/O module.**

  The IP address of the specified I/O module has been changed by the I/O module.

  Severity
  Informational

  Serviceable

No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0674

User Response
Information only; no action is required.

- **0EA1A003 : I/O module [arg1] IP address was changed to [arg2] by the I/O module.**

  The IP address of the specified I/O module has been changed by the I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0674

  User Response
  Information only; no action is required.

- **0EA1A004 : I/O module [arg1] IP address was changed to [arg2] by the I/O module.**

  The IP address of the specified I/O module has been changed by the I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0674

  User Response
  Information only; no action is required.

- **0EA1A401 : I/O module [arg1] current fault.**

  The power current for the specified I/O module has exceeded the fault threshold, and the I/O module will shut down. An I/O-module fault is also reported in the Chassis Management Module event log.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  I/O Modules (Critical)

  SNMP Trap ID
  mmTrapIOC

  CIM Information
  Prefix: CMM **ID:** 0049

  User Response
  Replace the I/O module.
- **0EA1A402 : I/O module [arg1] current fault.**

  The power current for the specified I/O module has exceeded the fault threshold, and the I/O module will shut down. An I/O-module fault is also reported in the Chassis Management Module event log.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  I/O Modules (Critical)

  SNMP Trap ID
  mmTrapIOC

  CIM Information
  Prefix: CMM **ID:** 0049

  User Response
  Replace the I/O module.
- **0EA1A403 : I/O module [arg1] current fault.**

  The power current for the specified I/O module has exceeded the fault threshold, and the I/O module will shut down. An I/O-module fault is also reported in the Chassis Management Module event log.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

Alert Category
I/O Modules (Critical)

SNMP Trap ID
mmTrapIOC

CIM Information
Prefix: CMM **ID:** 0049

User Response
Replace the I/O module.

- **0EA1A404 : I/O module [arg1] current fault.**

  The power current for the specified I/O module has exceeded the fault threshold, and the I/O module will shut down. An I/O-module fault is also reported in the Chassis Management Module event log.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  I/O Modules (Critical)

  SNMP Trap ID
  mmTrapIOC

  CIM Information
  Prefix: CMM **ID:** 0049

  User Response
  Replace the I/O module.

- **0EA1B001 : I/O module [arg1] NTP configuration pushed by MM was enabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has enabled the NTP configuration pushed by CMM for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0682

  User Response
  Information only; no action is required.

- **0EA1B002 : I/O module [arg1] NTP configuration pushed by MM was enabled by user ID [arg2] from [arg3] at IP address [arg4].**

The specified user has enabled the NTP configuration pushed by CMM for the specified I/O module.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0682

User Response
Information only; no action is required.

- **0EA1B003 : I/O module [arg1] NTP configuration pushed by MM was enabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has enabled the NTP configuration pushed by CMM for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0682

  User Response
  Information only; no action is required.

- **0EA1B004 : I/O module [arg1] NTP configuration pushed by MM was enabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has enabled the NTP configuration pushed by CMM for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0682

User Response
Information only; no action is required.

- **0EA1C001 : I/O module [arg1] NTP configuration pushed by MM was disabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has disabled the NTP configuration pushed by CMM for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0683

  User Response
  Information only; no action is required.

- **0EA1C002 : I/O module [arg1] NTP configuration pushed by MM was disabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has disabled the NTP configuration pushed by CMM for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0683

  User Response
  Information only; no action is required.

- **0EA1C003 : I/O module [arg1] NTP configuration pushed by MM was disabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has disabled the NTP configuration pushed by CMM for the specified I/O module.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0683

User Response
Information only; no action is required.

- **0EA1C004 : I/O module [arg1] NTP configuration pushed by MM was disabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has disabled the NTP configuration pushed by CMM for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0683

  User Response
  Information only; no action is required.

- **0EA1C401 : I/O module [arg1] temperature fault.**

  The temperature of the specified I/O module has exceeded the fault threshold, and the I/O module will shut down. The fan modules in the affected cooling zone will run at full speed.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  I/O Modules (Critical)

  SNMP Trap ID
  mmTrapIOC

CIM Information
Prefix: CMM **ID:** 0046

User Response
Complete the following steps until the problem is solved:

1. Check the Chassis Management Module event log for any events related to the fan modules, and solve those events.
2. Check the ambient room temperature to ensure that the room is not too hot.
3. Check for any blockage on or near the ventilation holes on the chassis. Remove any blockages that you find.
4. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that nothing is covering the bays. Empty bays can cause a reduction in airflow to the devices in the chassis.
5. Check the ambient chassis temperature. Make sure that enough fan modules are installed to sufficiently cool the devices in the chassis. See the chassis documentation to determine how many fan modules should be installed.

- **0EA1C402 : I/O module [arg1] temperature fault.**

The temperature of the specified I/O module has exceeded the fault threshold, and the I/O module will shut down. The fan modules in the affected cooling zone will run at full speed.

Severity
Error

Serviceable
Yes

Automatically notify support
No

Alert Category
I/O Modules (Critical)

SNMP Trap ID
mmTrapIOC

CIM Information
Prefix: CMM **ID:** 0046

User Response
Complete the following steps until the problem is solved:

1. Check the Chassis Management Module event log for any events related to the fan modules, and solve those events.
2. Check the ambient room temperature to ensure that the room is not too hot.
3. Check for any blockage on or near the ventilation holes on the chassis. Remove any blockages that you find.
4. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that nothing is covering the bays. Empty bays can cause a reduction in airflow to the devices in the chassis.
5. Check the ambient chassis temperature. Make sure that enough fan modules are installed to sufficiently cool the devices in the chassis. See the chassis documentation to determine how many fan modules should be installed.

- **0EA1C403 : I/O module [arg1] temperature fault.**

The temperature of the specified I/O module has exceeded the fault threshold, and the I/O module will shut down. The fan modules in the affected cooling zone will run at full speed.

Severity
Error

Serviceable
Yes

Automatically notify support
No

Alert Category
I/O Modules (Critical)

SNMP Trap ID
mmTrapIOC

CIM Information
Prefix: CMM **ID:** 0046

User Response
Complete the following steps until the problem is solved:

1. Check the Chassis Management Module event log for any events related to the fan modules, and solve those events.
2. Check the ambient room temperature to ensure that the room is not too hot.
3. Check for any blockage on or near the ventilation holes on the chassis. Remove any blockages that you find.
4. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that nothing is covering the bays. Empty bays can cause a reduction in airflow to the devices in the chassis.
5. Check the ambient chassis temperature. Make sure that enough fan modules are installed to sufficiently cool the devices in the chassis. See the chassis documentation to determine how many fan modules should be installed.

- **0EA1C404 : I/O module [arg1] temperature fault.**

The temperature of the specified I/O module has exceeded the fault threshold, and the I/O module will shut down. The fan modules in the affected cooling zone will run at full speed.

Severity
Error

Serviceable
Yes

Automatically notify support
No

Alert Category
I/O Modules (Critical)

SNMP Trap ID
mmTrapIOC

CIM Information
Prefix: CMM **ID:** 0046

User Response
Complete the following steps until the problem is solved:

1. Check the Chassis Management Module event log for any events related to the fan modules, and solve those events.
2. Check the ambient room temperature to ensure that the room is not too hot.

3. Check for any blockage on or near the ventilation holes on the chassis. Remove any blockages that you find.
4. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that nothing is covering the bays. Empty bays can cause a reduction in airflow to the devices in the chassis.
5. Check the ambient chassis temperature. Make sure that enough fan modules are installed to sufficiently cool the devices in the chassis. See the chassis documentation to determine how many fan modules should be installed.

- **0EA1D001 : I/O module [arg1] NTP update frequency was changed to [arg2] minutes by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the NTP update frequency of the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0684

  User Response
  Information only; no action is required.

- **0EA1D002 : I/O module [arg1] NTP update frequency was changed to [arg2] minutes by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the NTP update frequency of the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0684

  User Response
  Information only; no action is required.

- **0EA1D003 : I/O module [arg1] NTP update frequency was changed to [arg2] minutes by user ID [arg3] from [arg4] at IP address [arg5].**

The specified user has changed the NTP update frequency of the specified I/O module.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0684

User Response
Information only; no action is required.

- **0EA1D004 : I/O module [arg1] NTP update frequency was changed to [arg2] minutes by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the NTP update frequency of the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0684

  User Response
  Information only; no action is required.

- **0EA1D401 : I/O module [arg1] is over recommended temperature.**

  The temperature of the specified I/O module exceeds the recommended temperature.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  I/O Modules (Warning)

  SNMP Trap ID

mmTrapION

CIM Information
Prefix: CMM **ID:** 0047

User Response
Complete the following steps until the problem is solved:

1. Check the Chassis Management Module event log for any events related to the fan modules, and solve those events.
2. Check the ambient room temperature to ensure that the room is not too hot.
3. Check for any blockage on or near the ventilation holes on the chassis. Remove any blockages that you find.
4. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that nothing is covering the bays. Empty bays can cause a reduction in airflow to the devices in the chassis.
5. Check the ambient chassis temperature. Make sure that enough fan modules are installed to sufficiently cool the devices in the chassis. See the chassis documentation to determine how many fan modules should be installed.

- **0EA1D402 : I/O module [arg1] is over recommended temperature.**

The temperature of the specified I/O module exceeds the recommended temperature.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
I/O Modules (Warning)

SNMP Trap ID
mmTrapION

CIM Information
Prefix: CMM **ID:** 0047

User Response
Complete the following steps until the problem is solved:

1. Check the Chassis Management Module event log for any events related to the fan modules, and solve those events.
2. Check the ambient room temperature to ensure that the room is not too hot.
3. Check for any blockage on or near the ventilation holes on the chassis. Remove any blockages that you find.
4. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that nothing is covering the bays. Empty bays can cause a reduction in airflow to the devices in the chassis.
5. Check the ambient chassis temperature. Make sure that enough fan modules are installed to sufficiently cool the devices in the chassis. See the chassis documentation to determine how many fan modules should be installed.

- **0EA1D403 : I/O module [arg1] is over recommended temperature.**

The temperature of the specified I/O module exceeds the recommended temperature.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
I/O Modules (Warning)

SNMP Trap ID
mmTrapION

CIM Information
Prefix: CMM **ID:** 0047

User Response
Complete the following steps until the problem is solved:

1. Check the Chassis Management Module event log for any events related to the fan modules, and solve those events.
2. Check the ambient room temperature to ensure that the room is not too hot.
3. Check for any blockage on or near the ventilation holes on the chassis. Remove any blockages that you find.
4. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that nothing is covering the bays. Empty bays can cause a reduction in airflow to the devices in the chassis.
5. Check the ambient chassis temperature. Make sure that enough fan modules are installed to sufficiently cool the devices in the chassis. See the chassis documentation to determine how many fan modules should be installed.

- **0EA1D404 : I/O module [arg1] is over recommended temperature.**

The temperature of the specified I/O module exceeds the recommended temperature.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
I/O Modules (Warning)

SNMP Trap ID
mmTrapION

CIM Information
Prefix: CMM **ID:** 0047

User Response
Complete the following steps until the problem is solved:

1. Check the Chassis Management Module event log for any events related to the fan modules, and solve those events.
2. Check the ambient room temperature to ensure that the room is not too hot.

3. Check for any blockage on or near the ventilation holes on the chassis. Remove any blockages that you find.
4. Make sure that a device or filler is installed in each bay in the front and rear of the chassis, and make sure that nothing is covering the bays. Empty bays can cause a reduction in airflow to the devices in the chassis.
5. Check the ambient chassis temperature. Make sure that enough fan modules are installed to sufficiently cool the devices in the chassis. See the chassis documentation to determine how many fan modules should be installed.

- **0EA1E001 : I/O module [arg1] external management is disabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has modified the I/O module to disable external management.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0686

  User Response
  Information only; no action is required.

- **0EA1E002 : I/O module [arg1] external management is disabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has modified the I/O module to disable external management.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0686

  User Response
  Information only; no action is required.

- **0EA1E003 : I/O module [arg1] external management is disabled by user ID [arg2] from [arg3] at IP address [arg4].**

The specified user has modified the I/O module to disable external management.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0686

User Response
Information only; no action is required.

- **0EA1E004 : I/O module [arg1] external management is disabled by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has modified the I/O module to disable external management.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0686

  User Response
  Information only; no action is required.

- **0EA1F001 : I/O Module [arg1] stacking role transitioned from [arg2] to [arg3].**

  I/O module transitioned from one stacking role to another.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID

mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0690

User Response
Information only; no action is required.

- **0EA1F002 : I/O Module [arg1] stacking role transitioned from [arg2] to [arg3].**

  I/O module transitioned from one stacking role to another.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0690

  User Response
  Information only; no action is required.

- **0EA1F003 : I/O Module [arg1] stacking role transitioned from [arg2] to [arg3].**

  I/O module transitioned from one stacking role to another.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0690

  User Response
  Information only; no action is required.

- **0EA1F004 : I/O Module [arg1] stacking role transitioned from [arg2] to [arg3].**

  I/O module transitioned from one stacking role to another.

  Severity
  Informational

  Serviceable
  No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0690

User Response
Information only; no action is required.

- **0EA1F701 : I/O module [arg1] is not supported.**

The Chassis Management Module does not support the I/O module.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
I/O Modules (Warning)

SNMP Trap ID
mmTrapION

CIM Information
Prefix: CMM **ID:** 0326

User Response
Check the ServerProven list to make sure that the CMM supports the I/O module. Update the CMM firmware to a version that supports the I/O module.

- **0EA1F702 : I/O module [arg1] is not supported.**

The Chassis Management Module does not support the I/O module.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
I/O Modules (Warning)

SNMP Trap ID
mmTrapION

CIM Information
Prefix: CMM **ID:** 0326

User Response
Check the ServerProven list to make sure that the CMM supports the I/O module. Update the CMM firmware to a version that supports the I/O module.

- **0EA1F703 : I/O module [arg1] is not supported.**

  The Chassis Management Module does not support the I/O module.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  I/O Modules (Warning)

  SNMP Trap ID
  mmTrapION

  CIM Information
  Prefix: CMM **ID:** 0326

  User Response
  Check the ServerProven list to make sure that the CMM supports the I/O module. Update the CMM firmware to a version that supports the I/O module.
- **0EA1F704 : I/O module [arg1] is not supported.**

  The Chassis Management Module does not support the I/O module.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  I/O Modules (Warning)

  SNMP Trap ID
  mmTrapION

  CIM Information
  Prefix: CMM **ID:** 0326

  User Response
  Check the ServerProven list to make sure that the CMM supports the I/O module. Update the CMM firmware to a version that supports the I/O module.
- **0EA1F801 : I/O module [arg1] communication failure.**

  The Chassis Management Module fails to communicate with the I/O module.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category

I/O Modules (Warning)

SNMP Trap ID
mmTrapION

CIM Information
Prefix: CMM **ID:** 0329

User Response
Check the ServerProven list to make sure that the CMM supports the I/O module. Update the I/O firmware to a version that is supported. Reset or reseat I/O module.

- **0EA1F802 : I/O module [arg1] communication failure.**

The Chassis Management Module fails to communicate with the I/O module.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
I/O Modules (Warning)

SNMP Trap ID
mmTrapION

CIM Information
Prefix: CMM **ID:** 0329

User Response
Check the ServerProven list to make sure that the CMM supports the I/O module. Update the I/O firmware to a version that is supported. Reset or reseat I/O module.

- **0EA1F803 : I/O module [arg1] communication failure.**

The Chassis Management Module fails to communicate with the I/O module.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
I/O Modules (Warning)

SNMP Trap ID
mmTrapION

CIM Information
Prefix: CMM **ID:** 0329

User Response
Check the ServerProven list to make sure that the CMM supports the I/O module. Update the I/O firmware to a version that is supported. Reset or reseat I/O module.

- **0EA1F804 : I/O module [arg1] communication failure.**

The Chassis Management Module fails to communicate with the I/O module.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
I/O Modules (Warning)

SNMP Trap ID
mmTrapION

CIM Information
Prefix: CMM **ID:** 0329

User Response
Check the ServerProven list to make sure that the CMM supports the I/O module. Update the I/O firmware to a version that is supported. Reset or reseat I/O module.

- **0EA1F901 : [arg1] is isolated.**

RSIS notifies to isolate the specified I/O module. The specified I/O module powered on.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0785

User Response
Information only; no action is required.

- **0EA1F902 : [arg1] is isolated.**

RSIS notifies to isolate the specified I/O module. The specified I/O module powered on.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0785

User Response
Information only; no action is required.

- **0EA1F903 : [arg1] is isolated.**

RSIS notifies to isolate the specified I/O module. The specified I/O module powered on.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0785

User Response
Information only; no action is required.

- **0EA1F904 : [arg1] is isolated.**

RSIS notifies to isolate the specified I/O module. The specified I/O module powered on.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0785

User Response
Information only; no action is required.

- **0EA23001 : Service data collection initiated on [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

Service data collection initiated on specified I/O Module by the specified user.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0768

User Response
Information only; no action is required.

- **0EA23002 : Service data collection initiated on [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  Service data collection initiated on specified I/O Module by the specified user.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0768

  User Response
  Information only; no action is required.

- **0EA23003 : Service data collection initiated on [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  Service data collection initiated on specified I/O Module by the specified user.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0768

  User Response
  Information only; no action is required.

- **0EA23004 : Service data collection initiated on [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  Service data collection initiated on specified I/O Module by the specified user.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0768

  User Response
  Information only; no action is required.
- **0EA24001 : Service data collection completed on [arg1].**

  Service data collection completed on specified I/O Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0769

  User Response
  Information only; no action is required.
- **0EA24002 : Service data collection completed on [arg1].**

  Service data collection completed on specified I/O Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0769

User Response
Information only; no action is required.

- **0EA24003 : Service data collection completed on [arg1].**

  Service data collection completed on specified I/O Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0769

  User Response
  Information only; no action is required.

- **0EA24004 : Service data collection completed on [arg1].**

  Service data collection completed on specified I/O Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0769

  User Response
  Information only; no action is required.

- **0EA25001 : Service data collection failed on [arg1] with error code: [arg2].**

  Service data collection failed on specified I/O Module with the specified error code.

  Severity
  Warning

  Serviceable

No

Automatically notify support
No

Alert Category
I/O Modules (Warning)

SNMP Trap ID
mmTrapION

CIM Information
Prefix: CMM **ID:** 0852

User Response
Retry the I/O Module service data collection a few minutes after the intial failure. If the service data collection fails again, reset the I/O Module and try the I/O Module service data collection again. If the collection fails again, please contact Support.

- **0EA25002 : Service data collection failed on [arg1] with error code: [arg2].**

  Service data collection failed on specified I/O Module with the specified error code.

  Severity
  Warning

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Warning)

  SNMP Trap ID
  mmTrapION

  CIM Information
  Prefix: CMM **ID:** 0852

  User Response
  Retry the I/O Module service data collection a few minutes after the intial failure. If the service data collection fails again, reset the I/O Module and try the I/O Module service data collection again. If the collection fails again, please contact Support.

- **0EA25003 : Service data collection failed on [arg1] with error code: [arg2].**

  Service data collection failed on specified I/O Module with the specified error code.

  Severity
  Warning

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Warning)

  SNMP Trap ID
  mmTrapION

  CIM Information

Prefix: CMM **ID:** 0852

User Response
Retry the I/O Module service data collection a few minutes after the intial failure. If the service data collection fails again, reset the I/O Module and try the I/O Module service data collection again. If the collection fails again, please contact Support.

- **0EA25004 : Service data collection failed on [arg1] with error code: [arg2].**

Service data collection failed on specified I/O Module with the specified error code.

Severity
Warning

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Warning)

SNMP Trap ID
mmTrapION

CIM Information
Prefix: CMM **ID:** 0852

User Response
Retry the I/O Module service data collection a few minutes after the intial failure. If the service data collection fails again, reset the I/O Module and try the I/O Module service data collection again. If the collection fails again, please contact Support.

- **0EA26001 : I/O module [arg1] powered on.**

The specified I/O module powered on.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0783

User Response
Information only; no action is required.

- **0EA26002 : I/O module [arg1] powered on.**

The specified I/O module powered on.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0783

User Response
Information only; no action is required.

- **0EA26003 : I/O module [arg1] powered on.**

The specified I/O module powered on.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0783

User Response
Information only; no action is required.

- **0EA26004 : I/O module [arg1] powered on.**

The specified I/O module powered on.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0783

User Response

Information only; no action is required.

- **0EA27001 : I/O module [arg1] powered off.**

  The specified I/O module powered off.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0784

  User Response
  Information only; no action is required.

- **0EA27002 : I/O module [arg1] powered off.**

  The specified I/O module powered off.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0784

  User Response
  Information only; no action is required.

- **0EA27003 : I/O module [arg1] powered off.**

  The specified I/O module powered off.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0784

User Response
Information only; no action is required.

- **0EA27004 : I/O module [arg1] powered off.**

  The specified I/O module powered off.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0784

  User Response
  Information only; no action is required.

- **0EA28001 : I/O module [arg1] firmware image [arg2] set to be delay activated by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified fimrware image was set to be delay activated by the specified user.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0786

  User Response
  Information only; no action is required.

- **0EA28002 : I/O module [arg1] firmware image [arg2] set to be delay activated by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified fimrware image was set to be delay activated by the specified user.

  Severity

Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0786

User Response
Information only; no action is required.

- **0EA28003 : I/O module [arg1] firmware image [arg2] set to be delay activated by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified fimrware image was set to be delay activated by the specified user.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0786

  User Response
  Information only; no action is required.

- **0EA28004 : I/O module [arg1] firmware image [arg2] set to be delay activated by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified fimrware image was set to be delay activated by the specified user.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0786

User Response
Information only; no action is required.

- **0EA29001 : I/O module [arg1] firmware image [arg2] failed to accept user setting to delay activate by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified fimrware image failed to accept user setting to delay activate by the specified user.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0787

  User Response
  Retry the I/O Module firmware delayed activation a few minutes after the intial failure. If the delayed activation fails again, reset the I/O Module and try the I/O Module firmware delayed activation again. If the activation fails again, please contact Support.

- **0EA29002 : I/O module [arg1] firmware image [arg2] failed to accept user setting to delay activate by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified fimrware image failed to accept user setting to delay activate by the specified user.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0787

  User Response
  Retry the I/O Module firmware delayed activation a few minutes after the intial failure. If the delayed activation fails again, reset the I/O Module and try the I/O Module firmware delayed activation again. If the activation fails again, please contact Support.

- **0EA29003 : I/O module [arg1] firmware image [arg2] failed to accept user setting to delay activate by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified fimrware image failed to accept user setting to delay activate by the specified user.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0787

User Response
Retry the I/O Module firmware delayed activation a few minutes after the intial failure. If the delayed activation fails again, reset the I/O Module and try the I/O Module firmware delayed activation again. If the activation fails again, please contact Support.

- **0EA29004 : I/O module [arg1] firmware image [arg2] failed to accept user setting to delay activate by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified fimrware image failed to accept user setting to delay activate by the specified user.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0787

  User Response
  Retry the I/O Module firmware delayed activation a few minutes after the intial failure. If the delayed activation fails again, reset the I/O Module and try the I/O Module firmware delayed activation again. If the activation fails again, please contact Support.

- **0EA2A001 : I/O module [arg1] IP address [arg2] was set.**

  The IP address of the specified I/O module has been set.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category

I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0788

User Response
Information only; no action is required.

- **0EA2A002 : I/O module [arg1] IP address [arg2] was set.**

The IP address of the specified I/O module has been set.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0788

User Response
Information only; no action is required.

- **0EA2A003 : I/O module [arg1] IP address [arg2] was set.**

The IP address of the specified I/O module has been set.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0788

User Response
Information only; no action is required.

- **0EA2A004 : I/O module [arg1] IP address [arg2] was set.**

The IP address of the specified I/O module has been set.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0788

User Response
Information only; no action is required.

- **0EA2B001 : The internal proprietary management configuration for [arg1] succeeded.**

The Internal proprietary management configuration for I/O module succeeded.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0800

User Response
Information only; no action is required.

- **0EA2B002 : The internal proprietary management configuration for [arg1] succeeded.**

The Internal proprietary management configuration for I/O module succeeded.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0800

User Response

Information only; no action is required.

- **0EA2B003 : The internal proprietary management configuration for [arg1] succeeded.**

  The Internal proprietary management configuration for I/O module succeeded.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0800

  User Response
  Information only; no action is required.

- **0EA2B004 : The internal proprietary management configuration for [arg1] succeeded.**

  The Internal proprietary management configuration for I/O module succeeded.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0800

  User Response
  Information only; no action is required.

- **0EA2C001 : The internal proprietary management configuration for [arg1] failed.**

  The Internal proprietary management configuration for I/O module succeeded.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0801

User Response
Retry the I/O Module internal proprietay management configuration a few minutes after the intial failure. If fails again, reset the I/O Module and try again. If fails again, please contact Support.

- **0EA2C002 : The internal proprietary management configuration for [arg1] failed.**

The Internal proprietary management configuration for I/O module succeeded.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0801

User Response
Retry the I/O Module internal proprietay management configuration a few minutes after the intial failure. If fails again, reset the I/O Module and try again. If fails again, please contact Support.

- **0EA2C003 : The internal proprietary management configuration for [arg1] failed.**

The Internal proprietary management configuration for I/O module succeeded.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0801

User Response
Retry the I/O Module internal proprietay management configuration a few minutes after the intial failure. If fails again, reset the I/O Module and try again. If fails again, please contact Support.

- **0EA2C004 : The internal proprietary management configuration for [arg1] failed.**

The Internal proprietary management configuration for I/O module succeeded.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0801

User Response
Retry the I/O Module internal proprietay management configuration a few minutes after the intial failure. If fails again, reset the I/O Module and try again. If fails again, please contact Support.

- **0EA2D001 : The internal proprietary management credentials for [arg1] are incorrect with error code: [arg2].**

The Internal proprietary management configuration for I/O module are incorrect.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
I/O Modules (Warning)

SNMP Trap ID
mmTrapION

CIM Information
Prefix: CMM **ID:** 0802

User Response
Retry the I/O Module internal proprietay management configuration with correct information.

- **0EA2D002 : The internal proprietary management credentials for [arg1] are incorrect with error code: [arg2].**

The Internal proprietary management configuration for I/O module are incorrect.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
I/O Modules (Warning)

SNMP Trap ID

mmTrapION

CIM Information
Prefix: CMM **ID:** 0802

User Response
Retry the I/O Module internal proprietay management configuration with correct information.

- **0EA2D003 : The internal proprietary management credentials for [arg1] are incorrect with error code: [arg2].**

  The Internal proprietary management configuration for I/O module are incorrect.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  I/O Modules (Warning)

  SNMP Trap ID
  mmTrapION

  CIM Information
  Prefix: CMM **ID:** 0802

  User Response
  Retry the I/O Module internal proprietay management configuration with correct information.

- **0EA2D004 : The internal proprietary management credentials for [arg1] are incorrect with error code: [arg2].**

  The Internal proprietary management configuration for I/O module are incorrect.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  I/O Modules (Warning)

  SNMP Trap ID
  mmTrapION

  CIM Information
  Prefix: CMM **ID:** 0802

  User Response
  Retry the I/O Module internal proprietay management configuration with correct information.

- **0EA2E001 : Service data collection initiated on I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4] cannot be collected because device is power off.**

  Service data collection initiated on specified I/O Module by the specified user cannot be collected because device is power off.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0857

User Response
For taking service data collection on the specified I/O Module, please power on the device.

- **0EA2E002 : Service data collection initiated on I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4] cannot be collected because device is power off.**

  Service data collection initiated on specified I/O Module by the specified user cannot be collected because device is power off.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0857

  User Response
  For taking service data collection on the specified I/O Module, please power on the device.

- **0EA2E003 : Service data collection initiated on I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4] cannot be collected because device is power off.**

  Service data collection initiated on specified I/O Module by the specified user cannot be collected because device is power off.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0857

User Response
For taking service data collection on the specified I/O Module, please power on the device.

- **0EA2E004 : Service data collection initiated on I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4] cannot be collected because device is power off.**

  Service data collection initiated on specified I/O Module by the specified user cannot be collected because device is power off.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0857

  User Response
  For taking service data collection on the specified I/O Module, please power on the device.

- **0F00A001 : CMM failed to set the Fabric Manager configuration for node [arg1]. Node power permissions denied.**

  The Fabric Manager configuration cannot be applied to the specified node. Power permissions have been denied.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Critical)

  SNMP Trap ID
  mmTrapBladeC

  CIM Information
  Prefix: CMM **ID:** 1018

  User Response
  Complete the following steps until the problem is solved:

  1. Perform a service-level reset on the node.
  2. Update the firmware on the node through the system-management processor.

3. Update the firmware on the CMM.

- **0F00A002 : CMM failed to set the Fabric Manager configuration for node [arg1]. Node power permissions denied.**

  The Fabric Manager configuration cannot be applied to the specified node. Power permissions have been denied.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Critical)

  SNMP Trap ID
  mmTrapBladeC

  CIM Information
  Prefix: CMM **ID:** 1018

  User Response
  Complete the following steps until the problem is solved:

  1. Perform a service-level reset on the node.
  2. Update the firmware on the node through the system-management processor.
  3. Update the firmware on the CMM.

- **0F00A003 : CMM failed to set the Fabric Manager configuration for node [arg1]. Node power permissions denied.**

  The Fabric Manager configuration cannot be applied to the specified node. Power permissions have been denied.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Critical)

  SNMP Trap ID
  mmTrapBladeC

  CIM Information
  Prefix: CMM **ID:** 1018

  User Response
  Complete the following steps until the problem is solved:

  1. Perform a service-level reset on the node.
  2. Update the firmware on the node through the system-management processor.
  3. Update the firmware on the CMM.

- **0F00A004 : CMM failed to set the Fabric Manager configuration for node [arg1]. Node power permissions denied.**

  The Fabric Manager configuration cannot be applied to the specified node. Power permissions have been denied.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Critical)

  SNMP Trap ID
  mmTrapBladeC

  CIM Information
  Prefix: CMM **ID:** 1018

  User Response
  Complete the following steps until the problem is solved:

  1. Perform a service-level reset on the node.
  2. Update the firmware on the node through the system-management processor.
  3. Update the firmware on the CMM.

- **0F00A005 : CMM failed to set the Fabric Manager configuration for node [arg1]. Node power permissions denied.**

  The Fabric Manager configuration cannot be applied to the specified node. Power permissions have been denied.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Critical)

  SNMP Trap ID
  mmTrapBladeC

  CIM Information
  Prefix: CMM **ID:** 1018

  User Response
  Complete the following steps until the problem is solved:

  1. Perform a service-level reset on the node.
  2. Update the firmware on the node through the system-management processor.
  3. Update the firmware on the CMM.

- **0F00A006 : CMM failed to set the Fabric Manager configuration for node [arg1]. Node power permissions denied.**

The Fabric Manager configuration cannot be applied to the specified node. Power permissions have been denied.

Severity
Error

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 1018

User Response
Complete the following steps until the problem is solved:

1. Perform a service-level reset on the node.
2. Update the firmware on the node through the system-management processor.
3. Update the firmware on the CMM.

- **0F00A007 : CMM failed to set the Fabric Manager configuration for node [arg1]. Node power permissions denied.**

  The Fabric Manager configuration cannot be applied to the specified node. Power permissions have been denied.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Critical)

  SNMP Trap ID
  mmTrapBladeC

  CIM Information
  Prefix: CMM **ID:** 1018

  User Response
  Complete the following steps until the problem is solved:

  1. Perform a service-level reset on the node.
  2. Update the firmware on the node through the system-management processor.
  3. Update the firmware on the CMM.

- **0F00A008 : CMM failed to set the Fabric Manager configuration for node [arg1]. Node power permissions denied.**

  The Fabric Manager configuration cannot be applied to the specified node. Power permissions have been denied.

Severity
Error

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 1018

User Response
Complete the following steps until the problem is solved:

1. Perform a service-level reset on the node.
2. Update the firmware on the node through the system-management processor.
3. Update the firmware on the CMM.

- **0F00A009 : CMM failed to set the Fabric Manager configuration for node [arg1]. Node power permissions denied.**

  The Fabric Manager configuration cannot be applied to the specified node. Power permissions have been denied.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Critical)

  SNMP Trap ID
  mmTrapBladeC

  CIM Information
  Prefix: CMM **ID:** 1018

  User Response
  Complete the following steps until the problem is solved:

  1. Perform a service-level reset on the node.
  2. Update the firmware on the node through the system-management processor.
  3. Update the firmware on the CMM.

- **0F00A00A : CMM failed to set the Fabric Manager configuration for node [arg1]. Node power permissions denied.**

  The Fabric Manager configuration cannot be applied to the specified node. Power permissions have been denied.

  Severity
  Error

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 1018

User Response
Complete the following steps until the problem is solved:

1. Perform a service-level reset on the node.
2. Update the firmware on the node through the system-management processor.
3. Update the firmware on the CMM.

- **0F00A00B : CMM failed to set the Fabric Manager configuration for node [arg1]. Node power permissions denied.**

  The Fabric Manager configuration cannot be applied to the specified node. Power permissions have been denied.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Critical)

  SNMP Trap ID
  mmTrapBladeC

  CIM Information
  Prefix: CMM **ID:** 1018

  User Response
  Complete the following steps until the problem is solved:

  1. Perform a service-level reset on the node.
  2. Update the firmware on the node through the system-management processor.
  3. Update the firmware on the CMM.

- **0F00A00C : CMM failed to set the Fabric Manager configuration for node [arg1]. Node power permissions denied.**

  The Fabric Manager configuration cannot be applied to the specified node. Power permissions have been denied.

  Severity
  Error

  Serviceable
  Yes

Automatically notify support
No

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 1018

User Response
Complete the following steps until the problem is solved:

1. Perform a service-level reset on the node.
2. Update the firmware on the node through the system-management processor.
3. Update the firmware on the CMM.

- **0F00A00D : CMM failed to set the Fabric Manager configuration for node [arg1]. Node power permissions denied.**

  The Fabric Manager configuration cannot be applied to the specified node. Power permissions have been denied.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Critical)

  SNMP Trap ID
  mmTrapBladeC

  CIM Information
  Prefix: CMM **ID:** 1018

  User Response
  Complete the following steps until the problem is solved:

  1. Perform a service-level reset on the node.
  2. Update the firmware on the node through the system-management processor.
  3. Update the firmware on the CMM.

- **0F00A00E : CMM failed to set the Fabric Manager configuration for node [arg1]. Node power permissions denied.**

  The Fabric Manager configuration cannot be applied to the specified node. Power permissions have been denied.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 1018

User Response
Complete the following steps until the problem is solved:

1. Perform a service-level reset on the node.
2. Update the firmware on the node through the system-management processor.
3. Update the firmware on the CMM.

- **0F00B001 : Unable to apply Fabric Manager configuration to one or more devices at node [arg1].**

  Unable to apply Fabric Manager configuration to one or more devices at the specified node

  Severity
  Warning

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 1010

  User Response
  Chassis Management Module detected that Fabric Manager could not be applied to one or more devices at the specified node.

- **0F00B002 : Unable to apply Fabric Manager configuration to one or more devices at node [arg1].**

  Unable to apply Fabric Manager configuration to one or more devices at the specified node

  Severity
  Warning

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 1010

  User Response

Chassis Management Module detected that Fabric Manager could not be applied to one or more devices at the specified node.

- **0F00B003 : Unable to apply Fabric Manager configuration to one or more devices at node [arg1].**

  Unable to apply Fabric Manager configuration to one or more devices at the specified node

  Severity
  Warning

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 1010

  User Response
  Chassis Management Module detected that Fabric Manager could not be applied to one or more devices at the specified node.

- **0F00B004 : Unable to apply Fabric Manager configuration to one or more devices at node [arg1].**

  Unable to apply Fabric Manager configuration to one or more devices at the specified node

  Severity
  Warning

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 1010

  User Response
  Chassis Management Module detected that Fabric Manager could not be applied to one or more devices at the specified node.

- **0F00B005 : Unable to apply Fabric Manager configuration to one or more devices at node [arg1].**

  Unable to apply Fabric Manager configuration to one or more devices at the specified node

  Severity
  Warning

  Serviceable
  No

  Automatically notify support

No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 1010

User Response
Chassis Management Module detected that Fabric Manager could not be applied to one or more devices at the specified node.

- **0F00B006 : Unable to apply Fabric Manager configuration to one or more devices at node [arg1].**

  Unable to apply Fabric Manager configuration to one or more devices at the specified node

  Severity
  Warning

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 1010

  User Response
  Chassis Management Module detected that Fabric Manager could not be applied to one or more devices at the specified node.

- **0F00B007 : Unable to apply Fabric Manager configuration to one or more devices at node [arg1].**

  Unable to apply Fabric Manager configuration to one or more devices at the specified node

  Severity
  Warning

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 1010

  User Response
  Chassis Management Module detected that Fabric Manager could not be applied to one or more devices at the specified node.

- **0F00B008 : Unable to apply Fabric Manager configuration to one or more devices at node [arg1].**

  Unable to apply Fabric Manager configuration to one or more devices at the specified node

  Severity
  Warning

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 1010

  User Response
  Chassis Management Module detected that Fabric Manager could not be applied to one or more devices at the specified node.
- **0F00B009 : Unable to apply Fabric Manager configuration to one or more devices at node [arg1].**

  Unable to apply Fabric Manager configuration to one or more devices at the specified node

  Severity
  Warning

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 1010

  User Response
  Chassis Management Module detected that Fabric Manager could not be applied to one or more devices at the specified node.
- **0F00B00A : Unable to apply Fabric Manager configuration to one or more devices at node [arg1].**

  Unable to apply Fabric Manager configuration to one or more devices at the specified node

  Severity
  Warning

  Serviceable
  No

  Automatically notify support
  No

  Alert Category

Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 1010

User Response
Chassis Management Module detected that Fabric Manager could not be applied to one or more devices at the specified node.

- **0F00B00B : Unable to apply Fabric Manager configuration to one or more devices at node [arg1].**

  Unable to apply Fabric Manager configuration to one or more devices at the specified node

  Severity
  Warning

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 1010

  User Response
  Chassis Management Module detected that Fabric Manager could not be applied to one or more devices at the specified node.

- **0F00B00C : Unable to apply Fabric Manager configuration to one or more devices at node [arg1].**

  Unable to apply Fabric Manager configuration to one or more devices at the specified node

  Severity
  Warning

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 1010

  User Response
  Chassis Management Module detected that Fabric Manager could not be applied to one or more devices at the specified node.

- **0F00B00D : Unable to apply Fabric Manager configuration to one or more devices at node [arg1].**

  Unable to apply Fabric Manager configuration to one or more devices at the specified node

Severity
Warning

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 1010

User Response
Chassis Management Module detected that Fabric Manager could not be applied to one or more devices at the specified node.

- **0F00B00E : Unable to apply Fabric Manager configuration to one or more devices at node [arg1].**

  Unable to apply Fabric Manager configuration to one or more devices at the specified node

  Severity
  Warning

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 1010

  User Response
  Chassis Management Module detected that Fabric Manager could not be applied to one or more devices at the specified node.

- **0F00C001 : Node [arg1] not allowed to power on; constrained by power budget.**

  While the specified node is being powered on, the Chassis Management Module has detected that there is no longer enough capacity in the power budget to allow the node to continue powering on.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID

mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0822

User Response
Complete the following steps until the problem is solved:

1. Select a different power management policy to increase the power budget.
2. Install additional power supplies to increase the power capacity.
3. Individually remove lower-priority devices from the chassis until the power budget is sufficient.

- **0F00C002 : Node [arg1] not allowed to power on; constrained by power budget.**

  While the specified node is being powered on, the Chassis Management Module has detected that there is no longer enough capacity in the power budget to allow the node to continue powering on.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0822

  User Response
  Complete the following steps until the problem is solved:

  1. Select a different power management policy to increase the power budget.
  2. Install additional power supplies to increase the power capacity.
  3. Individually remove lower-priority devices from the chassis until the power budget is sufficient.

- **0F00C003 : Node [arg1] not allowed to power on; constrained by power budget.**

  While the specified node is being powered on, the Chassis Management Module has detected that there is no longer enough capacity in the power budget to allow the node to continue powering on.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0822

User Response

Complete the following steps until the problem is solved:

1. Select a different power management policy to increase the power budget.
2. Install additional power supplies to increase the power capacity.
3. Individually remove lower-priority devices from the chassis until the power budget is sufficient.

- **0F00C004 : Node [arg1] not allowed to power on; constrained by power budget.**

  While the specified node is being powered on, the Chassis Management Module has detected that there is no longer enough capacity in the power budget to allow the node to continue powering on.

  Severity

  Warning

  Serviceable

  Yes

  Automatically notify support

  No

  Alert Category

  Nodes (Warning)

  SNMP Trap ID

  mmTrapBladeN

  CIM Information

  Prefix: CMM **ID:** 0822

  User Response

  Complete the following steps until the problem is solved:

  1. Select a different power management policy to increase the power budget.
  2. Install additional power supplies to increase the power capacity.
  3. Individually remove lower-priority devices from the chassis until the power budget is sufficient.

- **0F00C005 : Node [arg1] not allowed to power on; constrained by power budget.**

  While the specified node is being powered on, the Chassis Management Module has detected that there is no longer enough capacity in the power budget to allow the node to continue powering on.

  Severity

  Warning

  Serviceable

  Yes

  Automatically notify support

  No

  Alert Category

  Nodes (Warning)

  SNMP Trap ID

  mmTrapBladeN

  CIM Information

  Prefix: CMM **ID:** 0822

  User Response

  Complete the following steps until the problem is solved:

  1. Select a different power management policy to increase the power budget.

2. Install additional power supplies to increase the power capacity.
3. Individually remove lower-priority devices from the chassis until the power budget is sufficient.

- **0F00C006 : Node [arg1] not allowed to power on; constrained by power budget.**

  While the specified node is being powered on, the Chassis Management Module has detected that there is no longer enough capacity in the power budget to allow the node to continue powering on.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0822

  User Response
  Complete the following steps until the problem is solved:

  1. Select a different power management policy to increase the power budget.
  2. Install additional power supplies to increase the power capacity.
  3. Individually remove lower-priority devices from the chassis until the power budget is sufficient.

- **0F00C007 : Node [arg1] not allowed to power on; constrained by power budget.**

  While the specified node is being powered on, the Chassis Management Module has detected that there is no longer enough capacity in the power budget to allow the node to continue powering on.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0822

  User Response
  Complete the following steps until the problem is solved:

  1. Select a different power management policy to increase the power budget.
  2. Install additional power supplies to increase the power capacity.
  3. Individually remove lower-priority devices from the chassis until the power budget is sufficient.

- **0F00C008 : Node [arg1] not allowed to power on; constrained by power budget.**

While the specified node is being powered on, the Chassis Management Module has detected that there is no longer enough capacity in the power budget to allow the node to continue powering on.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0822

User Response
Complete the following steps until the problem is solved:

1. Select a different power management policy to increase the power budget.
2. Install additional power supplies to increase the power capacity.
3. Individually remove lower-priority devices from the chassis until the power budget is sufficient.

- **0F00C009 : Node [arg1] not allowed to power on; constrained by power budget.**

While the specified node is being powered on, the Chassis Management Module has detected that there is no longer enough capacity in the power budget to allow the node to continue powering on.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0822

User Response
Complete the following steps until the problem is solved:

1. Select a different power management policy to increase the power budget.
2. Install additional power supplies to increase the power capacity.
3. Individually remove lower-priority devices from the chassis until the power budget is sufficient.

- **0F00C00A : Node [arg1] not allowed to power on; constrained by power budget.**

While the specified node is being powered on, the Chassis Management Module has detected that there is no longer enough capacity in the power budget to allow the node to continue powering on.

Severity

Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0822

User Response
Complete the following steps until the problem is solved:

1. Select a different power management policy to increase the power budget.
2. Install additional power supplies to increase the power capacity.
3. Individually remove lower-priority devices from the chassis until the power budget is sufficient.

- **0F00C00B : Node [arg1] not allowed to power on; constrained by power budget.**

  While the specified node is being powered on, the Chassis Management Module has detected that there is no longer enough capacity in the power budget to allow the node to continue powering on.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0822

  User Response
  Complete the following steps until the problem is solved:

  1. Select a different power management policy to increase the power budget.
  2. Install additional power supplies to increase the power capacity.
  3. Individually remove lower-priority devices from the chassis until the power budget is sufficient.

- **0F00C00C : Node [arg1] not allowed to power on; constrained by power budget.**

  While the specified node is being powered on, the Chassis Management Module has detected that there is no longer enough capacity in the power budget to allow the node to continue powering on.

  Severity
  Warning

  Serviceable
  Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0822

User Response
Complete the following steps until the problem is solved:

1. Select a different power management policy to increase the power budget.
2. Install additional power supplies to increase the power capacity.
3. Individually remove lower-priority devices from the chassis until the power budget is sufficient.

- **0F00C00D : Node [arg1] not allowed to power on; constrained by power budget.**

  While the specified node is being powered on, the Chassis Management Module has detected that there is no longer enough capacity in the power budget to allow the node to continue powering on.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0822

  User Response
  Complete the following steps until the problem is solved:

  1. Select a different power management policy to increase the power budget.
  2. Install additional power supplies to increase the power capacity.
  3. Individually remove lower-priority devices from the chassis until the power budget is sufficient.

- **0F00C00E : Node [arg1] not allowed to power on; constrained by power budget.**

  While the specified node is being powered on, the Chassis Management Module has detected that there is no longer enough capacity in the power budget to allow the node to continue powering on.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category

Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0822

User Response
Complete the following steps until the problem is solved:

1. Select a different power management policy to increase the power budget.
2. Install additional power supplies to increase the power capacity.
3. Individually remove lower-priority devices from the chassis until the power budget is sufficient.

- **0F00D001 : System firmware for [arg1] does not support Fabric Manager.**

The system firmware for the node does not support Fabric Manager . The Fabric Manager configuration cannot be applied to the specified node. The node can not be powered on because the Chassis Management Module will not grant permission to power on to the system-managment processor on the node.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 1015

User Response
If the node supports Fabric Manager, update the node system firmware with the latest level of firmware that supports Fabric Manager. If the node does not support Fabric Manager, then set the Fabric Manager mode off for this node. The system-management processor on the node must be restarted to disable Fabric Manager after Fabric Manager support has been disabled by the user.

- **0F00D002 : System firmware for [arg1] does not support Fabric Manager.**

The system firmware for the node does not support Fabric Manager . The Fabric Manager configuration cannot be applied to the specified node. The node can not be powered on because the Chassis Management Module will not grant permission to power on to the system-managment processor on the node.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 1015

User Response
If the node supports Fabric Manager, update the node system firmware with the latest level of firmware that supports Fabric Manager. If the node does not support Fabric Manager, then set the Fabric Manager mode off for this node. The system-management processor on the node must be restarted to disable Fabric Manager after Fabric Manager support has been disabled by the user.

- **0F00D003 : System firmware for [arg1] does not support Fabric Manager.**

The system firmware for the node does not support Fabric Manager . The Fabric Manager configuration cannot be applied to the specified node. The node can not be powered on because the Chassis Management Module will not grant permission to power on to the system-managment processor on the node.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 1015

User Response
If the node supports Fabric Manager, update the node system firmware with the latest level of firmware that supports Fabric Manager. If the node does not support Fabric Manager, then set the Fabric Manager mode off for this node. The system-management processor on the node must be restarted to disable Fabric Manager after Fabric Manager support has been disabled by the user.

- **0F00D004 : System firmware for [arg1] does not support Fabric Manager.**

The system firmware for the node does not support Fabric Manager . The Fabric Manager configuration cannot be applied to the specified node. The node can not be powered on because the Chassis Management Module will not grant permission to power on to the system-managment processor on the node.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 1015

User Response
If the node supports Fabric Manager, update the node system firmware with the latest level of firmware that supports Fabric Manager. If the node does not support Fabric Manager, then set the Fabric Manager mode off for this node. The system-management processor on the node must be restarted to disable Fabric Manager after Fabric Manager support has been disabled by the user.

- **0F00D005 : System firmware for [arg1] does not support Fabric Manager.**

The system firmware for the node does not support Fabric Manager . The Fabric Manager configuration cannot be applied to the specified node. The node can not be powered on because the Chassis Management Module will not grant permission to power on to the system-managment processor on the node.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 1015

User Response
If the node supports Fabric Manager, update the node system firmware with the latest level of firmware that supports Fabric Manager. If the node does not support Fabric Manager, then set the Fabric Manager mode off for this node. The system-management processor on the node must be restarted to disable Fabric Manager after Fabric Manager support has been disabled by the user.

- **0F00D006 : System firmware for [arg1] does not support Fabric Manager.**

The system firmware for the node does not support Fabric Manager . The Fabric Manager configuration cannot be applied to the specified node. The node can not be powered on because the Chassis Management Module will not grant permission to power on to the system-managment processor on the node.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 1015

User Response

If the node supports Fabric Manager, update the node system firmware with the latest level of firmware that supports Fabric Manager. If the node does not support Fabric Manager, then set the Fabric Manager mode off for this node. The system-management processor on the node must be restarted to disable Fabric Manager after Fabric Manager support has been disabled by the user.

- **0F00D007 : System firmware for [arg1] does not support Fabric Manager.**

The system firmware for the node does not support Fabric Manager . The Fabric Manager configuration cannot be applied to the specified node. The node can not be powered on because the Chassis Management Module will not grant permission to power on to the system-managment processor on the node.

Severity

Warning

Serviceable

Yes

Automatically notify support

No

Alert Category

Nodes (Warning)

SNMP Trap ID

mmTrapBladeN

CIM Information

Prefix: CMM **ID:** 1015

User Response

If the node supports Fabric Manager, update the node system firmware with the latest level of firmware that supports Fabric Manager. If the node does not support Fabric Manager, then set the Fabric Manager mode off for this node. The system-management processor on the node must be restarted to disable Fabric Manager after Fabric Manager support has been disabled by the user.

- **0F00D008 : System firmware for [arg1] does not support Fabric Manager.**

The system firmware for the node does not support Fabric Manager . The Fabric Manager configuration cannot be applied to the specified node. The node can not be powered on because the Chassis Management Module will not grant permission to power on to the system-managment processor on the node.

Severity

Warning

Serviceable

Yes

Automatically notify support

No

Alert Category

Nodes (Warning)

SNMP Trap ID

mmTrapBladeN

CIM Information

Prefix: CMM **ID:** 1015

User Response

If the node supports Fabric Manager, update the node system firmware with the latest level of firmware that supports Fabric Manager. If the node does not support Fabric Manager, then set the Fabric Manager mode off for this node. The system-management processor on the node must be restarted to disable Fabric Manager after Fabric Manager support has been disabled by the user.

- **0F00D009 : System firmware for [arg1] does not support Fabric Manager.**

  The system firmware for the node does not support Fabric Manager . The Fabric Manager configuration cannot be applied to the specified node. The node can not be powered on because the Chassis Management Module will not grant permission to power on to the system-managment processor on the node.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 1015

  User Response
  If the node supports Fabric Manager, update the node system firmware with the latest level of firmware that supports Fabric Manager. If the node does not support Fabric Manager, then set the Fabric Manager mode off for this node. The system-management processor on the node must be restarted to disable Fabric Manager after Fabric Manager support has been disabled by the user.

- **0F00D00A : System firmware for [arg1] does not support Fabric Manager.**

  The system firmware for the node does not support Fabric Manager . The Fabric Manager configuration cannot be applied to the specified node. The node can not be powered on because the Chassis Management Module will not grant permission to power on to the system-managment processor on the node.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 1015

  User Response
  If the node supports Fabric Manager, update the node system firmware with the latest level of firmware that supports Fabric Manager. If the node does not support Fabric Manager, then set the

Fabric Manager mode off for this node. The system-management processor on the node must be restarted to disable Fabric Manager after Fabric Manager support has been disabled by the user.

- **0F00D00B : System firmware for [arg1] does not support Fabric Manager.**

  The system firmware for the node does not support Fabric Manager . The Fabric Manager configuration cannot be applied to the specified node. The node can not be powered on because the Chassis Management Module will not grant permission to power on to the system-managment processor on the node.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 1015

  User Response
  If the node supports Fabric Manager, update the node system firmware with the latest level of firmware that supports Fabric Manager. If the node does not support Fabric Manager, then set the Fabric Manager mode off for this node. The system-management processor on the node must be restarted to disable Fabric Manager after Fabric Manager support has been disabled by the user.

- **0F00D00C : System firmware for [arg1] does not support Fabric Manager.**

  The system firmware for the node does not support Fabric Manager . The Fabric Manager configuration cannot be applied to the specified node. The node can not be powered on because the Chassis Management Module will not grant permission to power on to the system-managment processor on the node.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 1015

  User Response
  If the node supports Fabric Manager, update the node system firmware with the latest level of firmware that supports Fabric Manager. If the node does not support Fabric Manager, then set the Fabric Manager mode off for this node. The system-management processor on the node must be restarted to disable Fabric Manager after Fabric Manager support has been disabled by the user.

- **0F00D00D : System firmware for [arg1] does not support Fabric Manager.**

  The system firmware for the node does not support Fabric Manager . The Fabric Manager configuration cannot be applied to the specified node. The node can not be powered on because the Chassis Management Module will not grant permission to power on to the system-managment processor on the node.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 1015

  User Response
  If the node supports Fabric Manager, update the node system firmware with the latest level of firmware that supports Fabric Manager. If the node does not support Fabric Manager, then set the Fabric Manager mode off for this node. The system-management processor on the node must be restarted to disable Fabric Manager after Fabric Manager support has been disabled by the user.
- **0F00D00E : System firmware for [arg1] does not support Fabric Manager.**

  The system firmware for the node does not support Fabric Manager . The Fabric Manager configuration cannot be applied to the specified node. The node can not be powered on because the Chassis Management Module will not grant permission to power on to the system-managment processor on the node.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 1015

  User Response
  If the node supports Fabric Manager, update the node system firmware with the latest level of firmware that supports Fabric Manager. If the node does not support Fabric Manager, then set the Fabric Manager mode off for this node. The system-management processor on the node must be restarted to disable Fabric Manager after Fabric Manager support has been disabled by the user.
- **0F00E001 : An I/O device on [arg1] does not support Fabric Manager.**

An I/O device on the specified node does not support Fabric Manager. The Fabric Manager configuration cannot be applied to the specified node. The node can not be powered on because the Chassis Management Module will not grant permission to power on to the system-managment processor on the node.

Severity
Warning

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 1016

User Response
Verify that node supports Fabric Manager. If no Support, turn Fabric Manager mode off for this node. Restart the node to activate default behavior.

- **0F00E002 : An I/O device on [arg1] does not support Fabric Manager.**

An I/O device on the specified node does not support Fabric Manager. The Fabric Manager configuration cannot be applied to the specified node. The node can not be powered on because the Chassis Management Module will not grant permission to power on to the system-managment processor on the node.

Severity
Warning

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 1016

User Response
Verify that node supports Fabric Manager. If no Support, turn Fabric Manager mode off for this node. Restart the node to activate default behavior.

- **0F00E003 : An I/O device on [arg1] does not support Fabric Manager.**

An I/O device on the specified node does not support Fabric Manager. The Fabric Manager configuration cannot be applied to the specified node. The node can not be powered on because the Chassis Management Module will not grant permission to power on to the system-managment processor on the node.

Severity

Warning

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 1016

User Response
Verify that node supports Fabric Manager. If no Support, turn Fabric Manager mode off for this node. Restart the node to activate default behavior.

- **0F00E004 : An I/O device on [arg1] does not support Fabric Manager.**

An I/O device on the specified node does not support Fabric Manager. The Fabric Manager configuration cannot be applied to the specified node. The node can not be powered on because the Chassis Management Module will not grant permission to power on to the system-managment processor on the node.

Severity
Warning

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 1016

User Response
Verify that node supports Fabric Manager. If no Support, turn Fabric Manager mode off for this node. Restart the node to activate default behavior.

- **0F00E005 : An I/O device on [arg1] does not support Fabric Manager.**

An I/O device on the specified node does not support Fabric Manager. The Fabric Manager configuration cannot be applied to the specified node. The node can not be powered on because the Chassis Management Module will not grant permission to power on to the system-managment processor on the node.

Severity
Warning

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 1016

User Response
Verify that node supports Fabric Manager. If no Support, turn Fabric Manager mode off for this node. Restart the node to activate default behavior.

- **0F00E006 : An I/O device on [arg1] does not support Fabric Manager.**

An I/O device on the specified node does not support Fabric Manager. The Fabric Manager configuration cannot be applied to the specified node. The node can not be powered on because the Chassis Management Module will not grant permission to power on to the system-managment processor on the node.

Severity
Warning

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 1016

User Response
Verify that node supports Fabric Manager. If no Support, turn Fabric Manager mode off for this node. Restart the node to activate default behavior.

- **0F00E007 : An I/O device on [arg1] does not support Fabric Manager.**

An I/O device on the specified node does not support Fabric Manager. The Fabric Manager configuration cannot be applied to the specified node. The node can not be powered on because the Chassis Management Module will not grant permission to power on to the system-managment processor on the node.

Severity
Warning

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information

Prefix: CMM **ID:** 1016

User Response
Verify that node supports Fabric Manager. If no Support, turn Fabric Manager mode off for this node. Restart the node to activate default behavior.

- **0F00E008 : An I/O device on [arg1] does not support Fabric Manager.**

An I/O device on the specified node does not support Fabric Manager. The Fabric Manager configuration cannot be applied to the specified node. The node can not be powered on because the Chassis Management Module will not grant permission to power on to the system-managment processor on the node.

Severity
Warning

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 1016

User Response
Verify that node supports Fabric Manager. If no Support, turn Fabric Manager mode off for this node. Restart the node to activate default behavior.

- **0F00E009 : An I/O device on [arg1] does not support Fabric Manager.**

An I/O device on the specified node does not support Fabric Manager. The Fabric Manager configuration cannot be applied to the specified node. The node can not be powered on because the Chassis Management Module will not grant permission to power on to the system-managment processor on the node.

Severity
Warning

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 1016

User Response
Verify that node supports Fabric Manager. If no Support, turn Fabric Manager mode off for this node. Restart the node to activate default behavior.

- **0F00E00A : An I/O device on [arg1] does not support Fabric Manager.**

An I/O device on the specified node does not support Fabric Manager. The Fabric Manager configuration cannot be applied to the specified node. The node can not be powered on because the Chassis Management Module will not grant permission to power on to the system-managment processor on the node.

Severity
Warning

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 1016

User Response
Verify that node supports Fabric Manager. If no Support, turn Fabric Manager mode off for this node. Restart the node to activate default behavior.

- **0F00E00B : An I/O device on [arg1] does not support Fabric Manager.**

An I/O device on the specified node does not support Fabric Manager. The Fabric Manager configuration cannot be applied to the specified node. The node can not be powered on because the Chassis Management Module will not grant permission to power on to the system-managment processor on the node.

Severity
Warning

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 1016

User Response
Verify that node supports Fabric Manager. If no Support, turn Fabric Manager mode off for this node. Restart the node to activate default behavior.

- **0F00E00C : An I/O device on [arg1] does not support Fabric Manager.**

An I/O device on the specified node does not support Fabric Manager. The Fabric Manager configuration cannot be applied to the specified node. The node can not be powered on because the Chassis Management Module will not grant permission to power on to the system-managment processor on the node.

Severity

Warning

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 1016

User Response
Verify that node supports Fabric Manager. If no Support, turn Fabric Manager mode off for this node. Restart the node to activate default behavior.

- **0F00E00D : An I/O device on [arg1] does not support Fabric Manager.**

An I/O device on the specified node does not support Fabric Manager. The Fabric Manager configuration cannot be applied to the specified node. The node can not be powered on because the Chassis Management Module will not grant permission to power on to the system-managment processor on the node.

Severity
Warning

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 1016

User Response
Verify that node supports Fabric Manager. If no Support, turn Fabric Manager mode off for this node. Restart the node to activate default behavior.

- **0F00E00E : An I/O device on [arg1] does not support Fabric Manager.**

An I/O device on the specified node does not support Fabric Manager. The Fabric Manager configuration cannot be applied to the specified node. The node can not be powered on because the Chassis Management Module will not grant permission to power on to the system-managment processor on the node.

Severity
Warning

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 1016

User Response
Verify that node supports Fabric Manager. If no Support, turn Fabric Manager mode off for this node. Restart the node to activate default behavior.

- **0F00F001 : Communication problems between an Fabric Manager device and a storage target at node [arg1].**

  After the Fabric Manager settings have been applied to the node, the node cannot access the target storage device.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 1021

  User Response
  Verify the switch and storage device software and hardware configuration, including general connectivity and settings. Restart the node to activate settings.

- **0F00F002 : Communication problems between an Fabric Manager device and a storage target at node [arg1].**

  After the Fabric Manager settings have been applied to the node, the node cannot access the target storage device.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 1021

User Response
Verify the switch and storage device software and hardware configuration, including general connectivity and settings. Restart the node to activate settings.

- **0F00F003 : Communication problems between an Fabric Manager device and a storage target at node [arg1].**

  After the Fabric Manager settings have been applied to the node, the node cannot access the target storage device.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 1021

  User Response
  Verify the switch and storage device software and hardware configuration, including general connectivity and settings. Restart the node to activate settings.

- **0F00F004 : Communication problems between an Fabric Manager device and a storage target at node [arg1].**

  After the Fabric Manager settings have been applied to the node, the node cannot access the target storage device.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 1021

  User Response
  Verify the switch and storage device software and hardware configuration, including general connectivity and settings. Restart the node to activate settings.

- **0F00F005 : Communication problems between an Fabric Manager device and a storage target at node [arg1].**

  After the Fabric Manager settings have been applied to the node, the node cannot access the target storage device.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 1021

User Response
Verify the switch and storage device software and hardware configuration, including general connectivity and settings. Restart the node to activate settings.

- **0F00F006 : Communication problems between an Fabric Manager device and a storage target at node [arg1].**

  After the Fabric Manager settings have been applied to the node, the node cannot access the target storage device.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 1021

  User Response
  Verify the switch and storage device software and hardware configuration, including general connectivity and settings. Restart the node to activate settings.

- **0F00F007 : Communication problems between an Fabric Manager device and a storage target at node [arg1].**

  After the Fabric Manager settings have been applied to the node, the node cannot access the target storage device.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 1021

User Response
Verify the switch and storage device software and hardware configuration, including general connectivity and settings. Restart the node to activate settings.

- **0F00F008 : Communication problems between an Fabric Manager device and a storage target at node [arg1].**

  After the Fabric Manager settings have been applied to the node, the node cannot access the target storage device.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 1021

  User Response
  Verify the switch and storage device software and hardware configuration, including general connectivity and settings. Restart the node to activate settings.

- **0F00F009 : Communication problems between an Fabric Manager device and a storage target at node [arg1].**

  After the Fabric Manager settings have been applied to the node, the node cannot access the target storage device.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 1021

User Response
Verify the switch and storage device software and hardware configuration, including general connectivity and settings. Restart the node to activate settings.

- **0F00F00A : Communication problems between an Fabric Manager device and a storage target at node [arg1].**

  After the Fabric Manager settings have been applied to the node, the node cannot access the target storage device.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 1021

  User Response
  Verify the switch and storage device software and hardware configuration, including general connectivity and settings. Restart the node to activate settings.

- **0F00F00B : Communication problems between an Fabric Manager device and a storage target at node [arg1].**

  After the Fabric Manager settings have been applied to the node, the node cannot access the target storage device.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 1021

  User Response
  Verify the switch and storage device software and hardware configuration, including general connectivity and settings. Restart the node to activate settings.

- **0F00F00C : Communication problems between an Fabric Manager device and a storage target at node [arg1].**

  After the Fabric Manager settings have been applied to the node, the node cannot access the target storage device.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 1021

User Response
Verify the switch and storage device software and hardware configuration, including general connectivity and settings. Restart the node to activate settings.

- **0F00F00D : Communication problems between an Fabric Manager device and a storage target at node [arg1].**

  After the Fabric Manager settings have been applied to the node, the node cannot access the target storage device.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 1021

  User Response
  Verify the switch and storage device software and hardware configuration, including general connectivity and settings. Restart the node to activate settings.

- **0F00F00E : Communication problems between an Fabric Manager device and a storage target at node [arg1].**

  After the Fabric Manager settings have been applied to the node, the node cannot access the target storage device.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 1021

User Response
Verify the switch and storage device software and hardware configuration, including general connectivity and settings. Restart the node to activate settings.

- **0F010201 : CMM failed to read the Fabric Manager configuration from NVRAM for node [arg1]. Configuration data cleared. Physical addresses will be used.**

  The Fabric Manager configuration cannot be read from CMM NVRAM. Default physical addresses will be used.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 1020

  User Response
  Complete the following steps until the problem is solved:

  1. Restart the specified node.
  2. Perform a service-level reset on the CMM.
  3. Update the firmware on the CMM.

- **0F010202 : CMM failed to read the Fabric Manager configuration from NVRAM for node [arg1]. Configuration data cleared. Physical addresses will be used.**

  The Fabric Manager configuration cannot be read from CMM NVRAM. Default physical addresses will be used.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 1020

User Response
Complete the following steps until the problem is solved:

1. Restart the specified node.
2. Perform a service-level reset on the CMM.
3. Update the firmware on the CMM.

- **0F010203 : CMM failed to read the Fabric Manager configuration from NVRAM for node [arg1]. Configuration data cleared. Physical addresses will be used.**

  The Fabric Manager configuration cannot be read from CMM NVRAM. Default physical addresses will be used.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 1020

  User Response
  Complete the following steps until the problem is solved:

  1. Restart the specified node.
  2. Perform a service-level reset on the CMM.
  3. Update the firmware on the CMM.

- **0F010204 : CMM failed to read the Fabric Manager configuration from NVRAM for node [arg1]. Configuration data cleared. Physical addresses will be used.**

  The Fabric Manager configuration cannot be read from CMM NVRAM. Default physical addresses will be used.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 1020

User Response

Complete the following steps until the problem is solved:

1. Restart the specified node.
2. Perform a service-level reset on the CMM.
3. Update the firmware on the CMM.

- **0F010205 : CMM failed to read the Fabric Manager configuration from NVRAM for node [arg1]. Configuration data cleared. Physical addresses will be used.**

  The Fabric Manager configuration cannot be read from CMM NVRAM. Default physical addresses will be used.

  Severity

  Informational

  Serviceable

  No

  Automatically notify support

  No

  Alert Category

  Nodes (Informational)

  SNMP Trap ID

  mmTrapBladeS

  CIM Information

  Prefix: CMM **ID:** 1020

  User Response

  Complete the following steps until the problem is solved:

  1. Restart the specified node.
  2. Perform a service-level reset on the CMM.
  3. Update the firmware on the CMM.

- **0F010206 : CMM failed to read the Fabric Manager configuration from NVRAM for node [arg1]. Configuration data cleared. Physical addresses will be used.**

  The Fabric Manager configuration cannot be read from CMM NVRAM. Default physical addresses will be used.

  Severity

  Informational

  Serviceable

  No

  Automatically notify support

  No

  Alert Category

  Nodes (Informational)

  SNMP Trap ID

  mmTrapBladeS

  CIM Information

  Prefix: CMM **ID:** 1020

  User Response

  Complete the following steps until the problem is solved:

1. Restart the specified node.
2. Perform a service-level reset on the CMM.
3. Update the firmware on the CMM.

- **0F010207 : CMM failed to read the Fabric Manager configuration from NVRAM for node [arg1]. Configuration data cleared. Physical addresses will be used.**

  The Fabric Manager configuration cannot be read from CMM NVRAM. Default physical addresses will be used.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 1020

  User Response
  Complete the following steps until the problem is solved:

  1. Restart the specified node.
  2. Perform a service-level reset on the CMM.
  3. Update the firmware on the CMM.

- **0F010208 : CMM failed to read the Fabric Manager configuration from NVRAM for node [arg1]. Configuration data cleared. Physical addresses will be used.**

  The Fabric Manager configuration cannot be read from CMM NVRAM. Default physical addresses will be used.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 1020

  User Response
  Complete the following steps until the problem is solved:

  1. Restart the specified node.

2. Perform a service-level reset on the CMM.
3. Update the firmware on the CMM.

- **0F010209 : CMM failed to read the Fabric Manager configuration from NVRAM for node [arg1]. Configuration data cleared. Physical addresses will be used.**

  The Fabric Manager configuration cannot be read from CMM NVRAM. Default physical addresses will be used.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 1020

  User Response
  Complete the following steps until the problem is solved:

  1. Restart the specified node.
  2. Perform a service-level reset on the CMM.
  3. Update the firmware on the CMM.

- **0F01020A : CMM failed to read the Fabric Manager configuration from NVRAM for node [arg1]. Configuration data cleared. Physical addresses will be used.**

  The Fabric Manager configuration cannot be read from CMM NVRAM. Default physical addresses will be used.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 1020

  User Response
  Complete the following steps until the problem is solved:

  1. Restart the specified node.
  2. Perform a service-level reset on the CMM.

3. Update the firmware on the CMM.

- **0F01020B : CMM failed to read the Fabric Manager configuration from NVRAM for node [arg1]. Configuration data cleared. Physical addresses will be used.**

  The Fabric Manager configuration cannot be read from CMM NVRAM. Default physical addresses will be used.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 1020

  User Response
  Complete the following steps until the problem is solved:

  1. Restart the specified node.
  2. Perform a service-level reset on the CMM.
  3. Update the firmware on the CMM.

- **0F01020C : CMM failed to read the Fabric Manager configuration from NVRAM for node [arg1]. Configuration data cleared. Physical addresses will be used.**

  The Fabric Manager configuration cannot be read from CMM NVRAM. Default physical addresses will be used.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 1020

  User Response
  Complete the following steps until the problem is solved:

  1. Restart the specified node.
  2. Perform a service-level reset on the CMM.
  3. Update the firmware on the CMM.

- **0F01020D : CMM failed to read the Fabric Manager configuration from NVRAM for node [arg1]. Configuration data cleared. Physical addresses will be used.**

  The Fabric Manager configuration cannot be read from CMM NVRAM. Default physical addresses will be used.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 1020

  User Response
  Complete the following steps until the problem is solved:

  1. Restart the specified node.
  2. Perform a service-level reset on the CMM.
  3. Update the firmware on the CMM.

- **0F01020E : CMM failed to read the Fabric Manager configuration from NVRAM for node [arg1]. Configuration data cleared. Physical addresses will be used.**

  The Fabric Manager configuration cannot be read from CMM NVRAM. Default physical addresses will be used.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 1020

  User Response
  Complete the following steps until the problem is solved:

  1. Restart the specified node.
  2. Perform a service-level reset on the CMM.
  3. Update the firmware on the CMM.

- **0F501900 : Serial over LAN (SOL) Reset Sequence for [arg1] has been set to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

Serial over LAN (SOL) Retry Sequence has been changed for the specified node(s).

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0346

User Response
Information only; no action is required.

- **0F501A00 : Serial over LAN (SOL) Escape Sequence for [arg1] has been set to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  Serial over LAN (SOL) Escape Sequence has been changed for the specified node(s).

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0345

  User Response
  Information only; no action is required.

- **0F501B00 : Serial over LAN (SOL) Retry Interval for [arg1] has been set to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  Serial over LAN (SOL) Retry Interval has been changed for the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0344

User Response
Information only; no action is required.

- **0F501C00 : Serial over LAN (SOL) Retry Count for [arg1] has been set to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  Serial over LAN (SOL) Retry Count has been changed for the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0343

  User Response
  Information only; no action is required.

- **0F501D00 : Serial over LAN (SOL) Send Threshold for [arg1] has been set to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  Serial over LAN (SOL) Send Threshold has been changed for the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0342

  User Response
  Information only; no action is required.

- **0F501E00 : Serial over LAN (SOL) Accumulate Timeout for [arg1] has been set to [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  Serial over LAN (SOL) Accumulate Timeout has been changed for the specified node.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0341

User Response
Information only; no action is required.

- **0F501F00 : Serial over LAN (SOL) for [arg1] was enabled by user ID [arg2] from [arg3] at IP address [arg4].**

  Serial over LAN (SOL) has been enabled for the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0889

  User Response
  Information only; no action is required.

- **0F501F01 : Serial over LAN (SOL) for [arg1] was disabled by user ID [arg2] from [arg3] at IP address [arg4].**

  Serial over LAN (SOL) has been disabled for the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0890

User Response
Information only; no action is required.

- **0F501F02 : Serial over LAN (SOL) for all nodes was enabled by user ID [arg1] from [arg2] at IP address [arg3].**

  Serial over LAN (SOL) has been enabled globally for all nodes.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0891

  User Response
  Information only; no action is required.

- **0F501F03 : Serial over LAN (SOL) for all nodes was disabled by user ID [arg1] from [arg2] at IP address [arg3].**

  Serial over LAN (SOL) has been disabled globally for all nodes. Disabling SOL globally does not affect the SOL session status for each node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0892

  User Response
  Information only; no action is required.

- **1D000120 : Secure CIM-XML was enabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has enabled the secure CIM-XML port.

  Severity
  Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0928

User Response
Information only; no action is required.

- **1D020000 : LED [arg1] on device [arg2] state changed to [arg3].**

The specified LED has changed state.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0323

User Response
Information only; no action is required.

- **1D020100 : LED [arg1] on device [arg2] state changed to [arg3].**

The specified LED has changed state.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0323

User Response

Information only; no action is required.

- **1D020200 : LED [arg1] on device [arg2] state changed to [arg3].**

  The specified LED has changed state.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0323

  User Response
  Information only; no action is required.

- **1D020300 : LED [arg1] on device [arg2] state changed to [arg3].**

  The specified LED has changed state.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0323

  User Response
  Information only; no action is required.

- **1E00D001 : Fabric Manager configuration for node [arg1] was changed by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the Fabric Manager configuration in the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category

User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 1014

User Response
Information only; no action is required.

- **1E00D002 : Fabric Manager configuration for node [arg1] was changed by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the Fabric Manager configuration in the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 1014

  User Response
  Information only; no action is required.

- **1E00D003 : Fabric Manager configuration for node [arg1] was changed by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the Fabric Manager configuration in the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 1014

  User Response
  Information only; no action is required.

- **1E00D004 : Fabric Manager configuration for node [arg1] was changed by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the Fabric Manager configuration in the specified node.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 1014

User Response
Information only; no action is required.

- **1E00D005 : Fabric Manager configuration for node [arg1] was changed by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the Fabric Manager configuration in the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 1014

  User Response
  Information only; no action is required.

- **1E00D006 : Fabric Manager configuration for node [arg1] was changed by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the Fabric Manager configuration in the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 1014

User Response
Information only; no action is required.

- **1E00D007 : Fabric Manager configuration for node [arg1] was changed by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the Fabric Manager configuration in the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 1014

  User Response
  Information only; no action is required.

- **1E00D008 : Fabric Manager configuration for node [arg1] was changed by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the Fabric Manager configuration in the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 1014

  User Response
  Information only; no action is required.

- **1E00D009 : Fabric Manager configuration for node [arg1] was changed by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the Fabric Manager configuration in the specified node.

  Severity
  Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 1014

User Response
Information only; no action is required.

- **1E00D00A : Fabric Manager configuration for node [arg1] was changed by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the Fabric Manager configuration in the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 1014

  User Response
  Information only; no action is required.

- **1E00D00B : Fabric Manager configuration for node [arg1] was changed by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the Fabric Manager configuration in the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 1014

User Response
Information only; no action is required.

- **1E00D00C : Fabric Manager configuration for node [arg1] was changed by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the Fabric Manager configuration in the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 1014

  User Response
  Information only; no action is required.
- **1E00D00D : Fabric Manager configuration for node [arg1] was changed by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the Fabric Manager configuration in the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 1014

  User Response
  Information only; no action is required.
- **1E00D00E : Fabric Manager configuration for node [arg1] was changed by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the Fabric Manager configuration in the specified node.

  Severity
  Informational

  Serviceable
  No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 1014

User Response
Information only; no action is required.

- **1E00E001 : Fabric Manager configuration mismatch detected between the expected configuration and the actual configuration of node [arg1]. Expected configuration will take effect when the node is restarted.**

  The Fabric Manager configuration that the Chassis Management Module has detected does not match the configuration in the specified node. The active configuration in the specified node will be used.

  Severity
  Informational

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 1017

  User Response
  Verify the switch and storage device software and hardware configuration, including general connectivity and settings. Restart the node to apply the latest settings.

- **1E00E002 : Fabric Manager configuration mismatch detected between the expected configuration and the actual configuration of node [arg1]. Expected configuration will take effect when the node is restarted.**

  The Fabric Manager configuration that the Chassis Management Module has detected does not match the configuration in the specified node. The active configuration in the specified node will be used.

  Severity
  Informational

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 1017

User Response
Verify the switch and storage device software and hardware configuration, including general connectivity and settings. Restart the node to apply the latest settings.

- **1E00E003 : Fabric Manager configuration mismatch detected between the expected configuration and the actual configuration of node [arg1]. Expected configuration will take effect when the node is restarted.**

  The Fabric Manager configuration that the Chassis Management Module has detected does not match the configuration in the specified node. The active configuration in the specified node will be used.

  Severity
  Informational

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 1017

  User Response
  Verify the switch and storage device software and hardware configuration, including general connectivity and settings. Restart the node to apply the latest settings.

- **1E00E004 : Fabric Manager configuration mismatch detected between the expected configuration and the actual configuration of node [arg1]. Expected configuration will take effect when the node is restarted.**

  The Fabric Manager configuration that the Chassis Management Module has detected does not match the configuration in the specified node. The active configuration in the specified node will be used.

  Severity
  Informational

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 1017

  User Response
  Verify the switch and storage device software and hardware configuration, including general connectivity and settings. Restart the node to apply the latest settings.

- **1E00E005 : Fabric Manager configuration mismatch detected between the expected configuration and the actual configuration of node [arg1]. Expected configuration will take effect when the node is restarted.**

  The Fabric Manager configuration that the Chassis Management Module has detected does not match the configuration in the specified node. The active configuration in the specified node will be used.

  Severity
  Informational

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 1017

  User Response
  Verify the switch and storage device software and hardware configuration, including general connectivity and settings. Restart the node to apply the latest settings.
- **1E00E006 : Fabric Manager configuration mismatch detected between the expected configuration and the actual configuration of node [arg1]. Expected configuration will take effect when the node is restarted.**

  The Fabric Manager configuration that the Chassis Management Module has detected does not match the configuration in the specified node. The active configuration in the specified node will be used.

  Severity
  Informational

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 1017

  User Response
  Verify the switch and storage device software and hardware configuration, including general connectivity and settings. Restart the node to apply the latest settings.
- **1E00E007 : Fabric Manager configuration mismatch detected between the expected configuration and the actual configuration of node [arg1]. Expected configuration will take effect when the node is restarted.**

  The Fabric Manager configuration that the Chassis Management Module has detected does not match the configuration in the specified node. The active configuration in the specified node will be used.

Severity
Informational

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 1017

User Response
Verify the switch and storage device software and hardware configuration, including general connectivity and settings. Restart the node to apply the latest settings.

- **1E00E008 : Fabric Manager configuration mismatch detected between the expected configuration and the actual configuration of node [arg1]. Expected configuration will take effect when the node is restarted.**

  The Fabric Manager configuration that the Chassis Management Module has detected does not match the configuration in the specified node. The active configuration in the specified node will be used.

  Severity
  Informational

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 1017

  User Response
  Verify the switch and storage device software and hardware configuration, including general connectivity and settings. Restart the node to apply the latest settings.

- **1E00E009 : Fabric Manager configuration mismatch detected between the expected configuration and the actual configuration of node [arg1]. Expected configuration will take effect when the node is restarted.**

  The Fabric Manager configuration that the Chassis Management Module has detected does not match the configuration in the specified node. The active configuration in the specified node will be used.

  Severity
  Informational

  Serviceable
  Yes

  Automatically notify support

No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 1017

User Response
Verify the switch and storage device software and hardware configuration, including general connectivity and settings. Restart the node to apply the latest settings.

- **1E00E00A : Fabric Manager configuration mismatch detected between the expected configuration and the actual configuration of node [arg1]. Expected configuration will take effect when the node is restarted.**

  The Fabric Manager configuration that the Chassis Management Module has detected does not match the configuration in the specified node. The active configuration in the specified node will be used.

  Severity
  Informational

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 1017

  User Response
  Verify the switch and storage device software and hardware configuration, including general connectivity and settings. Restart the node to apply the latest settings.

- **1E00E00B : Fabric Manager configuration mismatch detected between the expected configuration and the actual configuration of node [arg1]. Expected configuration will take effect when the node is restarted.**

  The Fabric Manager configuration that the Chassis Management Module has detected does not match the configuration in the specified node. The active configuration in the specified node will be used.

  Severity
  Informational

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 1017

User Response
Verify the switch and storage device software and hardware configuration, including general connectivity and settings. Restart the node to apply the latest settings.

- **1E00E00C : Fabric Manager configuration mismatch detected between the expected configuration and the actual configuration of node [arg1]. Expected configuration will take effect when the node is restarted.**

  The Fabric Manager configuration that the Chassis Management Module has detected does not match the configuration in the specified node. The active configuration in the specified node will be used.

  Severity
  Informational

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 1017

  User Response
  Verify the switch and storage device software and hardware configuration, including general connectivity and settings. Restart the node to apply the latest settings.

- **1E00E00D : Fabric Manager configuration mismatch detected between the expected configuration and the actual configuration of node [arg1]. Expected configuration will take effect when the node is restarted.**

  The Fabric Manager configuration that the Chassis Management Module has detected does not match the configuration in the specified node. The active configuration in the specified node will be used.

  Severity
  Informational

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 1017

  User Response
  Verify the switch and storage device software and hardware configuration, including general connectivity and settings. Restart the node to apply the latest settings.

- **1E00E00E : Fabric Manager configuration mismatch detected between the expected configuration and the actual configuration of node [arg1]. Expected configuration will take effect when the node is restarted.**

  The Fabric Manager configuration that the Chassis Management Module has detected does not match the configuration in the specified node. The active configuration in the specified node will be used.

  Severity
  Informational

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 1017

  User Response
  Verify the switch and storage device software and hardware configuration, including general connectivity and settings. Restart the node to apply the latest settings.
- **1E00F001 : Node [arg1] system management processor does not support Fabric Manager.**

  The service processor on the specified device does not support Fabric Manager.

  Severity
  Warning

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 1012

  User Response
  Chassis Management Module detected that the service processor on the specified device does not support Fabric Manager.
- **1E00F002 : Node [arg1] system management processor does not support Fabric Manager.**

  The service processor on the specified device does not support Fabric Manager.

  Severity
  Warning

  Serviceable
  No

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 1012

User Response
Chassis Management Module detected that the service processor on the specified device does not support Fabric Manager.

- **1E00F003 : Node [arg1] system management processor does not support Fabric Manager.**

The service processor on the specified device does not support Fabric Manager.

Severity
Warning

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 1012

User Response
Chassis Management Module detected that the service processor on the specified device does not support Fabric Manager.

- **1E00F004 : Node [arg1] system management processor does not support Fabric Manager.**

The service processor on the specified device does not support Fabric Manager.

Severity
Warning

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 1012

User Response

Chassis Management Module detected that the service processor on the specified device does not support Fabric Manager.

- **1E00F005 : Node [arg1] system management processor does not support Fabric Manager.**

  The service processor on the specified device does not support Fabric Manager.

  Severity
  Warning

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 1012

  User Response
  Chassis Management Module detected that the service processor on the specified device does not support Fabric Manager.

- **1E00F006 : Node [arg1] system management processor does not support Fabric Manager.**

  The service processor on the specified device does not support Fabric Manager.

  Severity
  Warning

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 1012

  User Response
  Chassis Management Module detected that the service processor on the specified device does not support Fabric Manager.

- **1E00F007 : Node [arg1] system management processor does not support Fabric Manager.**

  The service processor on the specified device does not support Fabric Manager.

  Severity
  Warning

  Serviceable
  No

  Automatically notify support

No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 1012

User Response
Chassis Management Module detected that the service processor on the specified device does not support Fabric Manager.

- **1E00F008 : Node [arg1] system management processor does not support Fabric Manager.**

The service processor on the specified device does not support Fabric Manager.

Severity
Warning

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 1012

User Response
Chassis Management Module detected that the service processor on the specified device does not support Fabric Manager.

- **1E00F009 : Node [arg1] system management processor does not support Fabric Manager.**

The service processor on the specified device does not support Fabric Manager.

Severity
Warning

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 1012

User Response
Chassis Management Module detected that the service processor on the specified device does not support Fabric Manager.

- **1E00F00A : Node [arg1] system management processor does not support Fabric Manager.**

  The service processor on the specified device does not support Fabric Manager.

  Severity
  Warning

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 1012

  User Response
  Chassis Management Module detected that the service processor on the specified device does not support Fabric Manager.
- **1E00F00B : Node [arg1] system management processor does not support Fabric Manager.**

  The service processor on the specified device does not support Fabric Manager.

  Severity
  Warning

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 1012

  User Response
  Chassis Management Module detected that the service processor on the specified device does not support Fabric Manager.
- **1E00F00C : Node [arg1] system management processor does not support Fabric Manager.**

  The service processor on the specified device does not support Fabric Manager.

  Severity
  Warning

  Serviceable
  No

  Automatically notify support
  No

  Alert Category

Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 1012

User Response
Chassis Management Module detected that the service processor on the specified device does not support Fabric Manager.

- **1E00F00D : Node [arg1] system management processor does not support Fabric Manager.**

The service processor on the specified device does not support Fabric Manager.

Severity
Warning

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 1012

User Response
Chassis Management Module detected that the service processor on the specified device does not support Fabric Manager.

- **1E00F00E : Node [arg1] system management processor does not support Fabric Manager.**

The service processor on the specified device does not support Fabric Manager.

Severity
Warning

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 1012

User Response
Chassis Management Module detected that the service processor on the specified device does not support Fabric Manager.

- **1E00F00F : Fabric Manager configuration was cleared because the Chassis Management Module was moved to a new chassis or restored to default.**

The Fabric Manager configuration was cleared because the Chassis Management Module was moved to another chassis or restored to the default settings.

Severity
Informational

Serviceable
Yes

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 1023

User Response
Apply the Fabric Manager configuration.

- **35010000 : New Certificate Authority established by user ID [arg1] from [arg2] at IP address [arg3].**

The specified user has established a new digital certificate for the chassis Certificate Authority. Logon failures and communication failures might occur if the certificate is not distributed to devices that use the chassis Certificate Authority to authenticate the Chassis Management Module (CMM) or system-management processors. To distribute the certificate to the Flex System Manager management software, configure the Flex System Manager management software to manage the chassis after the new certificate has been established. To distribute the certificate to an external device such as an LDAP server, export the certificate from the CMM, and then import the certificate into the external device.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0400

User Response
Information only; no action is required.

- **35010001 : New Certificate Authority established.**

A new digital certificate has been established for the chassis Certificate Authority. Logon failures and communication failures might occur if the certificate is not distributed to devices that use the chassis Certificate Authority to authenticate the Chassis Management Module (CMM) or system-management processors. To distribute the certificate to the Flex System Manager management software, configure the Flex System Manager management software to manage the chassis after the new certificate has been established. To distribute the certificate to an external device such as an LDAP server, export the certificate from the CMM, and then import the certificate into the external device.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0401

User Response
Information only; no action is required.

- **35010002 : Certificate Authority issued a certificate with a subject common name of [arg1].**

  The chassis Certificate Authority has issued a digital certificate with the specified subject common name.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0403

  User Response
  Information only; no action is required.

- **35010008 : New Certificate Authority with common name [arg1] established by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has established a new digital certificate for the chassis Certificate Authority. Logon failures and communication failures might occur if the certificate is not distributed to devices that use the chassis Certificate Authority to authenticate the Chassis Management Module (CMM) or system-management processors. To distribute the certificate to the Flex System Manager management software, configure the Flex System Manager management software to manage the chassis after the new certificate has been established or export the certificate authority certificate and import the certificate into the FSM Certificate Trust Store. To distribute the certificate to an external device such as an LDAP server, export the certificate from the CMM, and then import the certificate into the external device.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support

No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0410

User Response
Information only; no action is required.

- **35010009 : New Certificate Authority with common name [arg1] established because the CMM was reset to defaults.**

  A new digital certificate has been established for the chassis Certificate Authority because the management module was reset to defaults. Logon failures and communication failures might occur if the certificate is not distributed to devices that use the chassis Certificate Authority to authenticate the Chassis Management Module (CMM) or system-management processors. To distribute the certificate to the Flex System Manager management software, configure the Flex System Manager management software to manage the chassis after the new certificate has been established or export the certificate authority certificate and import the certificate into the FSM Certificate Trust Store. To distribute the certificate to an external device such as an LDAP server, export the certificate from the CMM, and then import the certificate into the external device.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0411

  User Response
  Information only; no action is required.

- **3501000A : New Certificate Authority with common name [arg1] established during initial setup.**

  A new digital certificate has been established for the chassis Certificate Authority during initial setup of the management module. Logon failures and communication failures might occur if the certificate is not distributed to devices that use the chassis Certificate Authority to authenticate the Chassis Management Module (CMM) or system-management processors. To distribute the certificate to the Flex System Manager management software, configure the Flex System Manager management software to manage the chassis after the new certificate has been established or export the certificate authority certificate and import the certificate into the FSM Certificate Trust Store. To distribute the certificate to an external device such as an LDAP server, export the certificate from the CMM, and then import the certificate into the external device.

  Severity
  Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0412

User Response
Information only; no action is required.

- **3501000B : New Certificate Authority with common name [arg1] established because the chassis ID changed.**

  A new digital certificate has been established for the chassis Certificate Authority because the management module sensed a change in chassis identification or a change in ability to identify the chassis. Logon failures and communication failures might occur if the certificate is not distributed to devices that use the chassis Certificate Authority to authenticate the Chassis Management Module (CMM) or system-management processors. To distribute the certificate to the Flex System Manager management software, configure the Flex System Manager management software to manage the chassis after the new certificate has been established or export the certificate authority certificate and import the certificate into the FSM Certificate Trust Store. To distribute the certificate to an external device such as an LDAP server, export the certificate from the CMM, and then import the certificate into the external device.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0413

  User Response
  Information only; no action is required.

- **3501000C : New Certificate Authority with common name [arg1] established because the previous information was incomplete.**

  A new digital certificate has been established for the chassis Certificate Authority because previous certificate authority information was incomplete. Logon failures and communication failures might occur if the certificate is not distributed to devices that use the chassis Certificate Authority to authenticate the Chassis Management Module (CMM) or system-management processors. To distribute the certificate to the Flex System Manager management software, configure the Flex System Manager management software to manage the chassis after the new certificate has been established or export the certificate authority certificate and import the certificate into the FSM Certificate Trust Store. To distribute the

certificate to an external device such as an LDAP server, export the certificate from the CMM, and then import the certificate into the external device.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0414

User Response
Information only; no action is required.

- **350100A1 : Certificate Authority issued a certificate with a subject common name of [arg1] for node [arg2].**

  The chassis Certificate Authority has issued a digital certificate with the specified subject common name for the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0854

  User Response
  Information only; no action is required.

- **350100A2 : Certificate Authority issued a certificate with a subject common name of [arg1] for node [arg2].**

  The chassis Certificate Authority has issued a digital certificate with the specified subject common name for the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0854

User Response
Information only; no action is required.

- **350100A3 : Certificate Authority issued a certificate with a subject common name of [arg1] for node [arg2].**

  The chassis Certificate Authority has issued a digital certificate with the specified subject common name for the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0854

  User Response
  Information only; no action is required.

- **350100A4 : Certificate Authority issued a certificate with a subject common name of [arg1] for node [arg2].**

  The chassis Certificate Authority has issued a digital certificate with the specified subject common name for the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0854

  User Response
  Information only; no action is required.

- **350100A5 : Certificate Authority issued a certificate with a subject common name of [arg1] for node [arg2].**

  The chassis Certificate Authority has issued a digital certificate with the specified subject common name for the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0854

  User Response
  Information only; no action is required.
- **350100A6 : Certificate Authority issued a certificate with a subject common name of [arg1] for node [arg2].**

  The chassis Certificate Authority has issued a digital certificate with the specified subject common name for the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0854

  User Response
  Information only; no action is required.
- **350100A7 : Certificate Authority issued a certificate with a subject common name of [arg1] for node [arg2].**

  The chassis Certificate Authority has issued a digital certificate with the specified subject common name for the specified node.

  Severity
  Informational

  Serviceable
  No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0854

User Response
Information only; no action is required.

- **350100A8 : Certificate Authority issued a certificate with a subject common name of [arg1] for node [arg2].**

  The chassis Certificate Authority has issued a digital certificate with the specified subject common name for the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0854

  User Response
  Information only; no action is required.

- **350100A9 : Certificate Authority issued a certificate with a subject common name of [arg1] for node [arg2].**

  The chassis Certificate Authority has issued a digital certificate with the specified subject common name for the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0854

User Response
Information only; no action is required.

- **350100AA : Certificate Authority issued a certificate with a subject common name of [arg1] for node [arg2].**

  The chassis Certificate Authority has issued a digital certificate with the specified subject common name for the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0854

  User Response
  Information only; no action is required.

- **350100AB : Certificate Authority issued a certificate with a subject common name of [arg1] for node [arg2].**

  The chassis Certificate Authority has issued a digital certificate with the specified subject common name for the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0854

  User Response
  Information only; no action is required.

- **350100AC : Certificate Authority issued a certificate with a subject common name of [arg1] for node [arg2].**

  The chassis Certificate Authority has issued a digital certificate with the specified subject common name for the specified node.

  Severity
  Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0854

User Response
Information only; no action is required.

- **350100AD : Certificate Authority issued a certificate with a subject common name of [arg1] for node [arg2].**

  The chassis Certificate Authority has issued a digital certificate with the specified subject common name for the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0854

  User Response
  Information only; no action is required.

- **350100AE : Certificate Authority issued a certificate with a subject common name of [arg1] for node [arg2].**

  The chassis Certificate Authority has issued a digital certificate with the specified subject common name for the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0854

User Response
Information only; no action is required.

- **35010300 : Certificate Authority with common name [arg1] failed validation and requires regeneration.**

The resident Certificate Authority (CA) for the Chassis Management Module (CMM) has failed a self-test. The issue will likely be corrected by regenerating the CA. This failure can affect CMM communications with management applications (such as Flex System Manager - FSM), the CMM user interfaces, communications with end nodes, as well as other system-management functions.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0794

User Response
Regenerate the CA using either the CMM web-based user interface or the CMM command-line interface (CLI). The regeneration of the CA is a disruptive action and will have the following consequences:

1. The web servers on the CMM and all end nodes managed by CMM, will be restarted.
2. Any management applications, such as the FSM, will need to import the new CA into their trust store.
   – If you are using FSM, version 1.3.2 or earlier, download the CA root certificate from the CMM and import it into the certificate trust store on the FSM.
   – If you are using FSM, version 1.3.3 or later, use the FSM to repair CMM CA.
3. You must import the new CA root certificate into any web browser used to access CMM ,FSM and node UI's to avoid untrusted certificate errors in the browser.

- **35010400 : Security policy level changed to [arg1] (version [arg2]) by user ID [arg3] from [arg4] at IP address [arg5].**

The specified user has changed the security policy level for the chassis.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0420

User Response
Information only; no action is required.

- **35010401 : Security policy level changed to [arg1] (version [arg2]).**

  The security policy level for the chassis has been changed.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0421

  User Response
  Information only; no action is required.

- **35010411 : Security policy is in Pending state at system-management processor on [arg1].**

  The security policy is in Pending state at the specified system-management processor. You must reset the system-management processor for the change to take effect.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0424

  User Response
  Reset the system-management processor.

- **35010412 : Security policy is in Pending state at system-management processor on [arg1].**

  The security policy is in Pending state at the specified system-management processor. You must reset the system-management processor for the change to take effect.

  Severity

Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0424

User Response
Reset the system-management processor.

- **35010413 : Security policy is in Pending state at system-management processor on [arg1].**

  The security policy is in Pending state at the specified system-management processor. You must reset the system-management processor for the change to take effect.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0424

  User Response
  Reset the system-management processor.

- **35010414 : Security policy is in Pending state at system-management processor on [arg1].**

  The security policy is in Pending state at the specified system-management processor. You must reset the system-management processor for the change to take effect.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0424

User Response
Reset the system-management processor.

- **35010415 : Security policy is in Pending state at system-management processor on [arg1].**

  The security policy is in Pending state at the specified system-management processor. You must reset the system-management processor for the change to take effect.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0424

  User Response
  Reset the system-management processor.

- **35010416 : Security policy is in Pending state at system-management processor on [arg1].**

  The security policy is in Pending state at the specified system-management processor. You must reset the system-management processor for the change to take effect.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0424

  User Response
  Reset the system-management processor.

- **35010417 : Security policy is in Pending state at system-management processor on [arg1].**

  The security policy is in Pending state at the specified system-management processor. You must reset the system-management processor for the change to take effect.

  Severity
  Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0424

User Response
Reset the system-management processor.

- **35010418 : Security policy is in Pending state at system-management processor on [arg1].**

  The security policy is in Pending state at the specified system-management processor. You must reset the system-management processor for the change to take effect.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0424

  User Response
  Reset the system-management processor.

- **35010419 : Security policy is in Pending state at system-management processor on [arg1].**

  The security policy is in Pending state at the specified system-management processor. You must reset the system-management processor for the change to take effect.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0424

User Response
Reset the system-management processor.

- **3501041A : Security policy is in Pending state at system-management processor on [arg1].**

  The security policy is in Pending state at the specified system-management processor. You must reset the system-management processor for the change to take effect.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0424

  User Response
  Reset the system-management processor.

- **3501041B : Security policy is in Pending state at system-management processor on [arg1].**

  The security policy is in Pending state at the specified system-management processor. You must reset the system-management processor for the change to take effect.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0424

  User Response
  Reset the system-management processor.

- **3501041C : Security policy is in Pending state at system-management processor on [arg1].**

  The security policy is in Pending state at the specified system-management processor. You must reset the system-management processor for the change to take effect.

  Severity
  Warning

  Serviceable
  Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0424

User Response
Reset the system-management processor.

- **3501041D : Security policy is in Pending state at system-management processor on [arg1].**

  The security policy is in Pending state at the specified system-management processor. You must reset the system-management processor for the change to take effect.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0424

  User Response
  Reset the system-management processor.

- **3501041E : Security policy is in Pending state at system-management processor on [arg1].**

  The security policy is in Pending state at the specified system-management processor. You must reset the system-management processor for the change to take effect.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0424

  User Response
  Reset the system-management processor.

- **35010481 : Node [arg1] device [arg2][[arg3]] VPD is not valid.**

  The vital product data (VPD) of the specified device is not valid. VPD includes information such as the serial number and part number to uniquely identify the device.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0835

  User Response
  Replace the specified device.
- **35010482 : Node [arg1] device [arg2][[arg3]] VPD is not valid.**

  The vital product data (VPD) of the specified device is not valid. VPD includes information such as the serial number and part number to uniquely identify the device.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0835

  User Response
  Replace the specified device.
- **35010483 : Node [arg1] device [arg2][[arg3]] VPD is not valid.**

  The vital product data (VPD) of the specified device is not valid. VPD includes information such as the serial number and part number to uniquely identify the device.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0835

User Response
Replace the specified device.

- **35010484 : Node [arg1] device [arg2][[arg3]] VPD is not valid.**

  The vital product data (VPD) of the specified device is not valid. VPD includes information such as the serial number and part number to uniquely identify the device.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0835

  User Response
  Replace the specified device.
- **35010485 : Node [arg1] device [arg2][[arg3]] VPD is not valid.**

  The vital product data (VPD) of the specified device is not valid. VPD includes information such as the serial number and part number to uniquely identify the device.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0835

  User Response
  Replace the specified device.
- **35010486 : Node [arg1] device [arg2][[arg3]] VPD is not valid.**

The vital product data (VPD) of the specified device is not valid. VPD includes information such as the serial number and part number to uniquely identify the device.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0835

User Response
Replace the specified device.

- **35010487 : Node [arg1] device [arg2][[arg3]] VPD is not valid.**

The vital product data (VPD) of the specified device is not valid. VPD includes information such as the serial number and part number to uniquely identify the device.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0835

User Response
Replace the specified device.

- **35010488 : Node [arg1] device [arg2][[arg3]] VPD is not valid.**

The vital product data (VPD) of the specified device is not valid. VPD includes information such as the serial number and part number to uniquely identify the device.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category

Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0835

User Response
Replace the specified device.

- **35010489 : Node [arg1] device [arg2][[arg3]] VPD is not valid.**

  The vital product data (VPD) of the specified device is not valid. VPD includes information such as the serial number and part number to uniquely identify the device.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0835

  User Response
  Replace the specified device.

- **3501048A : Node [arg1] device [arg2][[arg3]] VPD is not valid.**

  The vital product data (VPD) of the specified device is not valid. VPD includes information such as the serial number and part number to uniquely identify the device.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0835

  User Response
  Replace the specified device.

- **3501048B : Node [arg1] device [arg2][[arg3]] VPD is not valid.**

  The vital product data (VPD) of the specified device is not valid. VPD includes information such as the serial number and part number to uniquely identify the device.

Severity
Warning

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0835

User Response
Replace the specified device.

- **3501048C : Node [arg1] device [arg2][[arg3]] VPD is not valid.**

  The vital product data (VPD) of the specified device is not valid. VPD includes information such as the serial number and part number to uniquely identify the device.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0835

  User Response
  Replace the specified device.

- **3501048D : Node [arg1] device [arg2][[arg3]] VPD is not valid.**

  The vital product data (VPD) of the specified device is not valid. VPD includes information such as the serial number and part number to uniquely identify the device.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0835

User Response
Replace the specified device.

- **3501048E : Node [arg1] device [arg2][[arg3]] VPD is not valid.**

  The vital product data (VPD) of the specified device is not valid. VPD includes information such as the serial number and part number to uniquely identify the device.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0835

  User Response
  Replace the specified device.

- **35010501 : CMM local authentication server will not use imported certificate until firmware on node [arg1] is updated to a version that supports imported certificates.**

  The system-management processor firmware level for the specified node does not support the use of imported SSL server certificates. The Chassis Management Module (CMM) is configured to use an imported SSL server certificate, and the system-management processor for the specified node does not support that configuration. The local authentication server will use a server certificate signed by the local Certificate Authority (CA). Note: for back-up purposes, the local authentication server on the CMM is always active, even though an external LDAP server may be used.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0798

  User Response
  Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the CMM. The CMM will begin using the imported server certificate for the local authentication server after the system-management processor firmware levels for all nodes

in the chassis have been updated, and the imported server certificate is re-applied via the CMM web UI:

1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
2. Select Re-Apply Installed Certificate.

- **35010502 : CMM local authentication server will not use imported certificate until firmware on node [arg1] is updated to a version that supports imported certificates.**

  The system-management processor firmware level for the specified node does not support the use of imported SSL server certificates. The Chassis Management Module (CMM) is configured to use an imported SSL server certificate, and the system-management processor for the specified node does not support that configuration. The local authentication server will use a server certificate signed by the local Certificate Authority (CA). Note: for back-up purposes, the local authentication server on the CMM is always active, even though an external LDAP server may be used.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0798

  User Response
  Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the CMM. The CMM will begin using the imported server certificate for the local authentication server after the system-management processor firmware levels for all nodes in the chassis have been updated, and the imported server certificate is re-applied via the CMM web UI:

  1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
  2. Select Re-Apply Installed Certificate.

- **35010503 : CMM local authentication server will not use imported certificate until firmware on node [arg1] is updated to a version that supports imported certificates.**

  The system-management processor firmware level for the specified node does not support the use of imported SSL server certificates. The Chassis Management Module (CMM) is configured to use an imported SSL server certificate, and the system-management processor for the specified node does not support that configuration. The local authentication server will use a server certificate signed by the local Certificate Authority (CA). Note: for back-up purposes, the local authentication server on the CMM is always active, even though an external LDAP server may be used.

  Severity
  Informational

  Serviceable
  No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0798

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the CMM. The CMM will begin using the imported server certificate for the local authentication server after the system-management processor firmware levels for all nodes in the chassis have been updated, and the imported server certificate is re-applied via the CMM web UI:

1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
2. Select Re-Apply Installed Certificate.

- **35010504 : CMM local authentication server will not use imported certificate until firmware on node [arg1] is updated to a version that supports imported certificates.**

The system-management processor firmware level for the specified node does not support the use of imported SSL server certificates. The Chassis Management Module (CMM) is configured to use an imported SSL server certificate, and the system-management processor for the specified node does not support that configuration. The local authentication server will use a server certificate signed by the local Certificate Authority (CA). Note: for back-up purposes, the local authentication server on the CMM is always active, even though an external LDAP server may be used.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0798

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the CMM. The CMM will begin using the imported server certificate for the local authentication server after the system-management processor firmware levels for all nodes in the chassis have been updated, and the imported server certificate is re-applied via the CMM web UI:

1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
2. Select Re-Apply Installed Certificate.

- **35010505 : CMM local authentication server will not use imported certificate until firmware on node [arg1] is updated to a version that supports imported certificates.**

  The system-management processor firmware level for the specified node does not support the use of imported SSL server certificates. The Chassis Management Module (CMM) is configured to use an imported SSL server certificate, and the system-management processor for the specified node does not support that configuration. The local authentication server will use a server certificate signed by the local Certificate Authority (CA). Note: for back-up purposes, the local authentication server on the CMM is always active, even though an external LDAP server may be used.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0798

  User Response
  Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the CMM. The CMM will begin using the imported server certificate for the local authentication server after the system-management processor firmware levels for all nodes in the chassis have been updated, and the imported server certificate is re-applied via the CMM web UI:

  1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
  2. Select Re-Apply Installed Certificate.

- **35010506 : CMM local authentication server will not use imported certificate until firmware on node [arg1] is updated to a version that supports imported certificates.**

  The system-management processor firmware level for the specified node does not support the use of imported SSL server certificates. The Chassis Management Module (CMM) is configured to use an imported SSL server certificate, and the system-management processor for the specified node does not support that configuration. The local authentication server will use a server certificate signed by the local Certificate Authority (CA). Note: for back-up purposes, the local authentication server on the CMM is always active, even though an external LDAP server may be used.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID

mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0798

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the CMM. The CMM will begin using the imported server certificate for the local authentication server after the system-management processor firmware levels for all nodes in the chassis have been updated, and the imported server certificate is re-applied via the CMM web UI:

1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
2. Select Re-Apply Installed Certificate.

- **35010507 : CMM local authentication server will not use imported certificate until firmware on node [arg1] is updated to a version that supports imported certificates.**

The system-management processor firmware level for the specified node does not support the use of imported SSL server certificates. The Chassis Management Module (CMM) is configured to use an imported SSL server certificate, and the system-management processor for the specified node does not support that configuration. The local authentication server will use a server certificate signed by the local Certificate Authority (CA). Note: for back-up purposes, the local authentication server on the CMM is always active, even though an external LDAP server may be used.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0798

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the CMM. The CMM will begin using the imported server certificate for the local authentication server after the system-management processor firmware levels for all nodes in the chassis have been updated, and the imported server certificate is re-applied via the CMM web UI:

1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
2. Select Re-Apply Installed Certificate.

- **35010508 : CMM local authentication server will not use imported certificate until firmware on node [arg1] is updated to a version that supports imported certificates.**

The system-management processor firmware level for the specified node does not support the use of imported SSL server certificates. The Chassis Management Module (CMM) is configured to use an imported SSL server certificate, and the system-management processor for the specified node does not support that configuration. The local authentication server will use a server certificate signed by the local

Certificate Authority (CA). Note: for back-up purposes, the local authentication server on the CMM is always active, even though an external LDAP server may be used.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0798

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the CMM. The CMM will begin using the imported server certificate for the local authentication server after the system-management processor firmware levels for all nodes in the chassis have been updated, and the imported server certificate is re-applied via the CMM web UI:

1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
2. Select Re-Apply Installed Certificate.

- **35010509 : CMM local authentication server will not use imported certificate until firmware on node [arg1] is updated to a version that supports imported certificates.**

The system-management processor firmware level for the specified node does not support the use of imported SSL server certificates. The Chassis Management Module (CMM) is configured to use an imported SSL server certificate, and the system-management processor for the specified node does not support that configuration. The local authentication server will use a server certificate signed by the local Certificate Authority (CA). Note: for back-up purposes, the local authentication server on the CMM is always active, even though an external LDAP server may be used.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0798

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the CMM. The CMM will begin using the imported server certificate for

the local authentication server after the system-management processor firmware levels for all nodes in the chassis have been updated, and the imported server certificate is re-applied via the CMM web UI:

1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
2. Select Re-Apply Installed Certificate.

- **3501050A : CMM local authentication server will not use imported certificate until firmware on node [arg1] is updated to a version that supports imported certificates.**

  The system-management processor firmware level for the specified node does not support the use of imported SSL server certificates. The Chassis Management Module (CMM) is configured to use an imported SSL server certificate, and the system-management processor for the specified node does not support that configuration. The local authentication server will use a server certificate signed by the local Certificate Authority (CA). Note: for back-up purposes, the local authentication server on the CMM is always active, even though an external LDAP server may be used.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0798

  User Response
  Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the CMM. The CMM will begin using the imported server certificate for the local authentication server after the system-management processor firmware levels for all nodes in the chassis have been updated, and the imported server certificate is re-applied via the CMM web UI:

  1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
  2. Select Re-Apply Installed Certificate.

- **3501050B : CMM local authentication server will not use imported certificate until firmware on node [arg1] is updated to a version that supports imported certificates.**

  The system-management processor firmware level for the specified node does not support the use of imported SSL server certificates. The Chassis Management Module (CMM) is configured to use an imported SSL server certificate, and the system-management processor for the specified node does not support that configuration. The local authentication server will use a server certificate signed by the local Certificate Authority (CA). Note: for back-up purposes, the local authentication server on the CMM is always active, even though an external LDAP server may be used.

  Severity
  Informational

  Serviceable
  No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0798

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the CMM. The CMM will begin using the imported server certificate for the local authentication server after the system-management processor firmware levels for all nodes in the chassis have been updated, and the imported server certificate is re-applied via the CMM web UI:

1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
2. Select Re-Apply Installed Certificate.

- **3501050C : CMM local authentication server will not use imported certificate until firmware on node [arg1] is updated to a version that supports imported certificates.**

The system-management processor firmware level for the specified node does not support the use of imported SSL server certificates. The Chassis Management Module (CMM) is configured to use an imported SSL server certificate, and the system-management processor for the specified node does not support that configuration. The local authentication server will use a server certificate signed by the local Certificate Authority (CA). Note: for back-up purposes, the local authentication server on the CMM is always active, even though an external LDAP server may be used.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0798

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the CMM. The CMM will begin using the imported server certificate for the local authentication server after the system-management processor firmware levels for all nodes in the chassis have been updated, and the imported server certificate is re-applied via the CMM web UI:

1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
2. Select Re-Apply Installed Certificate.

- **3501050D : CMM local authentication server will not use imported certificate until firmware on node [arg1] is updated to a version that supports imported certificates.**

  The system-management processor firmware level for the specified node does not support the use of imported SSL server certificates. The Chassis Management Module (CMM) is configured to use an imported SSL server certificate, and the system-management processor for the specified node does not support that configuration. The local authentication server will use a server certificate signed by the local Certificate Authority (CA). Note: for back-up purposes, the local authentication server on the CMM is always active, even though an external LDAP server may be used.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0798

  User Response
  Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the CMM. The CMM will begin using the imported server certificate for the local authentication server after the system-management processor firmware levels for all nodes in the chassis have been updated, and the imported server certificate is re-applied via the CMM web UI:

  1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
  2. Select Re-Apply Installed Certificate.

- **3501050E : CMM local authentication server will not use imported certificate until firmware on node [arg1] is updated to a version that supports imported certificates.**

  The system-management processor firmware level for the specified node does not support the use of imported SSL server certificates. The Chassis Management Module (CMM) is configured to use an imported SSL server certificate, and the system-management processor for the specified node does not support that configuration. The local authentication server will use a server certificate signed by the local Certificate Authority (CA). Note: for back-up purposes, the local authentication server on the CMM is always active, even though an external LDAP server may be used.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID

mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0798

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the CMM. The CMM will begin using the imported server certificate for the local authentication server after the system-management processor firmware levels for all nodes in the chassis have been updated, and the imported server certificate is re-applied via the CMM web UI:

1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
2. Select Re-Apply Installed Certificate.

- **35010600 : Chassis Management Module local authentication server is now using the imported certificate.**

The local authentication server on the Chassis Management Module (CMM) is now using the imported server certificate. Note: for back-up purposes, the local authentication server on the CMM is always active, even though an external LDAP server may be used.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0799

User Response
Information only; no action is required.

- **35010701 : The UUID for node [arg1] is not unique in the chassis.**

The Chassis Management Module has detected that there are two or more nodes in the chassis that have duplicate universally unique identifier (UUID) values stored in their vital product data (VPD). The Chassis Management Module requires that this value is unique for all nodes in the chassis. The existence of duplicate UUID's will result in issues discovering and powering on the affected nodes.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID

mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0780

User Response
Contact your hardware service provider for assistance in correcting any duplicate UUID's.

- **35010702 : The UUID for node [arg1] is not unique in the chassis.**

The Chassis Management Module has detected that there are two or more nodes in the chassis that have duplicate universally unique identifier (UUID) values stored in their vital product data (VPD). The Chassis Management Module requires that this value is unique for all nodes in the chassis. The existence of duplicate UUID's will result in issues discovering and powering on the affected nodes.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0780

User Response
Contact your hardware service provider for assistance in correcting any duplicate UUID's.

- **35010703 : The UUID for node [arg1] is not unique in the chassis.**

The Chassis Management Module has detected that there are two or more nodes in the chassis that have duplicate universally unique identifier (UUID) values stored in their vital product data (VPD). The Chassis Management Module requires that this value is unique for all nodes in the chassis. The existence of duplicate UUID's will result in issues discovering and powering on the affected nodes.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0780

User Response
Contact your hardware service provider for assistance in correcting any duplicate UUID's.

- **35010704 : The UUID for node [arg1] is not unique in the chassis.**

The Chassis Management Module has detected that there are two or more nodes in the chassis that have duplicate universally unique identifier (UUID) values stored in their vital product data (VPD). The Chassis Management Module requires that this value is unique for all nodes in the chassis. The existence of duplicate UUID's will result in issues discovering and powering on the affected nodes.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0780

User Response
Contact your hardware service provider for assistance in correcting any duplicate UUID's.

- **35010705 : The UUID for node [arg1] is not unique in the chassis.**

The Chassis Management Module has detected that there are two or more nodes in the chassis that have duplicate universally unique identifier (UUID) values stored in their vital product data (VPD). The Chassis Management Module requires that this value is unique for all nodes in the chassis. The existence of duplicate UUID's will result in issues discovering and powering on the affected nodes.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0780

User Response
Contact your hardware service provider for assistance in correcting any duplicate UUID's.

- **35010706 : The UUID for node [arg1] is not unique in the chassis.**

The Chassis Management Module has detected that there are two or more nodes in the chassis that have duplicate universally unique identifier (UUID) values stored in their vital product data (VPD). The Chassis Management Module requires that this value is unique for all nodes in the chassis. The existence of duplicate UUID's will result in issues discovering and powering on the affected nodes.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0780

User Response
Contact your hardware service provider for assistance in correcting any duplicate UUID's.

- **35010707 : The UUID for node [arg1] is not unique in the chassis.**

The Chassis Management Module has detected that there are two or more nodes in the chassis that have duplicate universally unique identifier (UUID) values stored in their vital product data (VPD). The Chassis Management Module requires that this value is unique for all nodes in the chassis. The existence of duplicate UUID's will result in issues discovering and powering on the affected nodes.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0780

User Response
Contact your hardware service provider for assistance in correcting any duplicate UUID's.

- **35010708 : The UUID for node [arg1] is not unique in the chassis.**

The Chassis Management Module has detected that there are two or more nodes in the chassis that have duplicate universally unique identifier (UUID) values stored in their vital product data (VPD). The Chassis Management Module requires that this value is unique for all nodes in the chassis. The existence of duplicate UUID's will result in issues discovering and powering on the affected nodes.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0780

User Response
Contact your hardware service provider for assistance in correcting any duplicate UUID's.

- **35010709 : The UUID for node [arg1] is not unique in the chassis.**

  The Chassis Management Module has detected that there are two or more nodes in the chassis that have duplicate universally unique identifier (UUID) values stored in their vital product data (VPD). The Chassis Management Module requires that this value is unique for all nodes in the chassis. The existence of duplicate UUID's will result in issues discovering and powering on the affected nodes.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0780

  User Response
  Contact your hardware service provider for assistance in correcting any duplicate UUID's.

- **3501070A : The UUID for node [arg1] is not unique in the chassis.**

  The Chassis Management Module has detected that there are two or more nodes in the chassis that have duplicate universally unique identifier (UUID) values stored in their vital product data (VPD). The Chassis Management Module requires that this value is unique for all nodes in the chassis. The existence of duplicate UUID's will result in issues discovering and powering on the affected nodes.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0780

  User Response
  Contact your hardware service provider for assistance in correcting any duplicate UUID's.

- **3501070B : The UUID for node [arg1] is not unique in the chassis.**

The Chassis Management Module has detected that there are two or more nodes in the chassis that have duplicate universally unique identifier (UUID) values stored in their vital product data (VPD). The Chassis Management Module requires that this value is unique for all nodes in the chassis. The existence of duplicate UUID's will result in issues discovering and powering on the affected nodes.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0780

User Response
Contact your hardware service provider for assistance in correcting any duplicate UUID's.

- **3501070C : The UUID for node [arg1] is not unique in the chassis.**

The Chassis Management Module has detected that there are two or more nodes in the chassis that have duplicate universally unique identifier (UUID) values stored in their vital product data (VPD). The Chassis Management Module requires that this value is unique for all nodes in the chassis. The existence of duplicate UUID's will result in issues discovering and powering on the affected nodes.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0780

User Response
Contact your hardware service provider for assistance in correcting any duplicate UUID's.

- **3501070D : The UUID for node [arg1] is not unique in the chassis.**

The Chassis Management Module has detected that there are two or more nodes in the chassis that have duplicate universally unique identifier (UUID) values stored in their vital product data (VPD). The Chassis Management Module requires that this value is unique for all nodes in the chassis. The existence of duplicate UUID's will result in issues discovering and powering on the affected nodes.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0780

User Response
Contact your hardware service provider for assistance in correcting any duplicate UUID's.

- **3501070E : The UUID for node [arg1] is not unique in the chassis.**

The Chassis Management Module has detected that there are two or more nodes in the chassis that have duplicate universally unique identifier (UUID) values stored in their vital product data (VPD). The Chassis Management Module requires that this value is unique for all nodes in the chassis. The existence of duplicate UUID's will result in issues discovering and powering on the affected nodes.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0780

User Response
Contact your hardware service provider for assistance in correcting any duplicate UUID's.

- **35010801 : Unexpected exception affecting [arg1] was encountered in security service.**

An internal exception occurred in the security service of the Chassis Management Module (CMM). The specified node might not power on. You might not be able to log in to the system-management processor. The Flex System Manager management software might not be able to communicate with the system-management processor. Support will address this software issue and must engage Product Engineering, who will engage Development. CMM service data is required.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0404

User Response
Support will address this issue and must engage Product Engineering. Complete the following steps as a workaround until the problem is solved:

1. Make sure that the CMM has the correct level of firmware. Check the firmware change history for security updates.
2. Reset the primary CMM.

No hardware components have to be replaced.

- **35010802 : Unexpected exception affecting [arg1] was encountered in security service.**

An internal exception occurred in the security service of the Chassis Management Module (CMM). The specified node might not power on. You might not be able to log in to the system-management processor. The Flex System Manager management software might not be able to communicate with the system-management processor. Support will address this software issue and must engage Product Engineering, who will engage Development. CMM service data is required.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0404

User Response
Support will address this issue and must engage Product Engineering. Complete the following steps as a workaround until the problem is solved:

1. Make sure that the CMM has the correct level of firmware. Check the firmware change history for security updates.
2. Reset the primary CMM.

No hardware components have to be replaced.

- **35010803 : Unexpected exception affecting [arg1] was encountered in security service.**

An internal exception occurred in the security service of the Chassis Management Module (CMM). The specified node might not power on. You might not be able to log in to the system-management processor. The Flex System Manager management software might not be able to communicate with the system-management processor. Support will address this software issue and must engage Product Engineering, who will engage Development. CMM service data is required.

Severity
Error

Serviceable

Yes

Automatically notify support
Yes

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0404

User Response
Support will address this issue and must engage Product Engineering. Complete the following steps as a workaround until the problem is solved:

1. Make sure that the CMM has the correct level of firmware. Check the firmware change history for security updates.
2. Reset the primary CMM.

No hardware components have to be replaced.

- **35010804 : Unexpected exception affecting [arg1] was encountered in security service.**

An internal exception occurred in the security service of the Chassis Management Module (CMM). The specified node might not power on. You might not be able to log in to the system-management processor. The Flex System Manager management software might not be able to communicate with the system-management processor. Support will address this software issue and must engage Product Engineering, who will engage Development. CMM service data is required.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0404

User Response
Support will address this issue and must engage Product Engineering. Complete the following steps as a workaround until the problem is solved:

1. Make sure that the CMM has the correct level of firmware. Check the firmware change history for security updates.
2. Reset the primary CMM.

No hardware components have to be replaced.

- **35010805 : Unexpected exception affecting [arg1] was encountered in security service.**

An internal exception occurred in the security service of the Chassis Management Module (CMM). The specified node might not power on. You might not be able to log in to the system-management processor. The Flex System Manager management software might not be able to communicate with the system-

management processor. Support will address this software issue and must engage Product Engineering, who will engage Development. CMM service data is required.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0404

User Response
Support will address this issue and must engage Product Engineering. Complete the following steps as a workaround until the problem is solved:

1. Make sure that the CMM has the correct level of firmware. Check the firmware change history for security updates.
2. Reset the primary CMM.

No hardware components have to be replaced.

- **35010806 : Unexpected exception affecting [arg1] was encountered in security service.**

An internal exception occurred in the security service of the Chassis Management Module (CMM). The specified node might not power on. You might not be able to log in to the system-management processor. The Flex System Manager management software might not be able to communicate with the system-management processor. Support will address this software issue and must engage Product Engineering, who will engage Development. CMM service data is required.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0404

User Response
Support will address this issue and must engage Product Engineering. Complete the following steps as a workaround until the problem is solved:

1. Make sure that the CMM has the correct level of firmware. Check the firmware change history for security updates.

2. Reset the primary CMM.

No hardware components have to be replaced.

- **35010807 : Unexpected exception affecting [arg1] was encountered in security service.**

An internal exception occurred in the security service of the Chassis Management Module (CMM). The specified node might not power on. You might not be able to log in to the system-management processor. The Flex System Manager management software might not be able to communicate with the system-management processor. Support will address this software issue and must engage Product Engineering, who will engage Development. CMM service data is required.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0404

User Response
Support will address this issue and must engage Product Engineering. Complete the following steps as a workaround until the problem is solved:

1. Make sure that the CMM has the correct level of firmware. Check the firmware change history for security updates.
2. Reset the primary CMM.

No hardware components have to be replaced.

- **35010808 : Unexpected exception affecting [arg1] was encountered in security service.**

An internal exception occurred in the security service of the Chassis Management Module (CMM). The specified node might not power on. You might not be able to log in to the system-management processor. The Flex System Manager management software might not be able to communicate with the system-management processor. Support will address this software issue and must engage Product Engineering, who will engage Development. CMM service data is required.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0404

User Response

Support will address this issue and must engage Product Engineering. Complete the following steps as a workaround until the problem is solved:

1. Make sure that the CMM has the correct level of firmware. Check the firmware change history for security updates.
2. Reset the primary CMM.

No hardware components have to be replaced.

- **35010809 : Unexpected exception affecting [arg1] was encountered in security service.**

An internal exception occurred in the security service of the Chassis Management Module (CMM). The specified node might not power on. You might not be able to log in to the system-management processor. The Flex System Manager management software might not be able to communicate with the system-management processor. Support will address this software issue and must engage Product Engineering, who will engage Development. CMM service data is required.

Severity

Error

Serviceable

Yes

Automatically notify support

Yes

Alert Category

Nodes (Critical)

SNMP Trap ID

mmTrapBladeC

CIM Information

Prefix: CMM **ID:** 0404

User Response

Support will address this issue and must engage Product Engineering. Complete the following steps as a workaround until the problem is solved:

1. Make sure that the CMM has the correct level of firmware. Check the firmware change history for security updates.
2. Reset the primary CMM.

No hardware components have to be replaced.

- **3501080A : Unexpected exception affecting [arg1] was encountered in security service.**

An internal exception occurred in the security service of the Chassis Management Module (CMM). The specified node might not power on. You might not be able to log in to the system-management processor. The Flex System Manager management software might not be able to communicate with the system-management processor. Support will address this software issue and must engage Product Engineering, who will engage Development. CMM service data is required.

Severity

Error

Serviceable

Yes

Automatically notify support

Yes

Alert Category

Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0404

User Response
Support will address this issue and must engage Product Engineering. Complete the following steps as a workaround until the problem is solved:

1. Make sure that the CMM has the correct level of firmware. Check the firmware change history for security updates.
2. Reset the primary CMM.

No hardware components have to be replaced.

- **3501080B : Unexpected exception affecting [arg1] was encountered in security service.**

An internal exception occurred in the security service of the Chassis Management Module (CMM). The specified node might not power on. You might not be able to log in to the system-management processor. The Flex System Manager management software might not be able to communicate with the system-management processor. Support will address this software issue and must engage Product Engineering, who will engage Development. CMM service data is required.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0404

User Response
Support will address this issue and must engage Product Engineering. Complete the following steps as a workaround until the problem is solved:

1. Make sure that the CMM has the correct level of firmware. Check the firmware change history for security updates.
2. Reset the primary CMM.

No hardware components have to be replaced.

- **3501080C : Unexpected exception affecting [arg1] was encountered in security service.**

An internal exception occurred in the security service of the Chassis Management Module (CMM). The specified node might not power on. You might not be able to log in to the system-management processor. The Flex System Manager management software might not be able to communicate with the system-management processor. Support will address this software issue and must engage Product Engineering, who will engage Development. CMM service data is required.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0404

User Response
Support will address this issue and must engage Product Engineering. Complete the following steps as a workaround until the problem is solved:

1. Make sure that the CMM has the correct level of firmware. Check the firmware change history for security updates.
2. Reset the primary CMM.

No hardware components have to be replaced.

- **3501080D : Unexpected exception affecting [arg1] was encountered in security service.**

An internal exception occurred in the security service of the Chassis Management Module (CMM). The specified node might not power on. You might not be able to log in to the system-management processor. The Flex System Manager management software might not be able to communicate with the system-management processor. Support will address this software issue and must engage Product Engineering, who will engage Development. CMM service data is required.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0404

User Response
Support will address this issue and must engage Product Engineering. Complete the following steps as a workaround until the problem is solved:

1. Make sure that the CMM has the correct level of firmware. Check the firmware change history for security updates.
2. Reset the primary CMM.

No hardware components have to be replaced.

- **3501080E : Unexpected exception affecting [arg1] was encountered in security service.**

An internal exception occurred in the security service of the Chassis Management Module (CMM). The specified node might not power on. You might not be able to log in to the system-management processor.

The Flex System Manager management software might not be able to communicate with the system-management processor. Support will address this software issue and must engage Product Engineering, who will engage Development. CMM service data is required.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0404

User Response
Support will address this issue and must engage Product Engineering. Complete the following steps as a workaround until the problem is solved:

1. Make sure that the CMM has the correct level of firmware. Check the firmware change history for security updates.
2. Reset the primary CMM.

No hardware components have to be replaced.

- **35010841 : Unexpected exception was encountered in security service or system-management processor on [arg1].**

An internal exception occurred in the security service of the Chassis Management Module (CMM) or in the specified system-management processor. The specified node might not power on. You might not be able to log in to the system-management processor. The Flex System Manager management software might not be able to communicate with the system-management processor. Support will address this software issue and must engage Product Engineering, who will engage Development. CMM and node service data is required.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0406

User Response
Complete the following steps as a workaround until the problem is solved:

1. Make sure that the CMM and the affected node have the correct level of firmware.

2. Check the firmware change history for security updates.
3. To manually retry the operation, reset the affected system-management processor on the node. If you cannot reset the system-management processor from the Flex System Manager management software, reset it from the CMM. If you have problems resetting the affected system-management processor, perform a service-level reset of the node. Note that a service-level reset will shut down the operating system.
4. If the error remains after the system-management processor is reset, reset the primary CMM.

No hardware components have to be replaced.

- **35010842 : Unexpected exception was encountered in security service or system-management processor on [arg1].**

  An internal exception occurred in the security service of the Chassis Management Module (CMM) or in the specified system-management processor. The specified node might not power on. You might not be able to log in to the system-management processor. The Flex System Manager management software might not be able to communicate with the system-management processor. Support will address this software issue and must engage Product Engineering, who will engage Development. CMM and node service data is required.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Nodes (Critical)

  SNMP Trap ID
  mmTrapBladeC

  CIM Information
  Prefix: CMM **ID:** 0406

  User Response
  Complete the following steps as a workaround until the problem is solved:

  1. Make sure that the CMM and the affected node have the correct level of firmware.
  2. Check the firmware change history for security updates.
  3. To manually retry the operation, reset the affected system-management processor on the node. If you cannot reset the system-management processor from the Flex System Manager management software, reset it from the CMM. If you have problems resetting the affected system-management processor, perform a service-level reset of the node. Note that a service-level reset will shut down the operating system.
  4. If the error remains after the system-management processor is reset, reset the primary CMM.

  No hardware components have to be replaced.

- **35010843 : Unexpected exception was encountered in security service or system-management processor on [arg1].**

  An internal exception occurred in the security service of the Chassis Management Module (CMM) or in the specified system-management processor. The specified node might not power on. You might not be able to log in to the system-management processor. The Flex System Manager management software might not be able to communicate with the system-management processor. Support will address this software issue and must engage Product Engineering, who will engage Development. CMM and node service data is required.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0406

User Response
Complete the following steps as a workaround until the problem is solved:

1. Make sure that the CMM and the affected node have the correct level of firmware.
2. Check the firmware change history for security updates.
3. To manually retry the operation, reset the affected system-management processor on the node. If you cannot reset the system-management processor from the Flex System Manager management software, reset it from the CMM. If you have problems resetting the affected system-management processor, perform a service-level reset of the node. Note that a service-level reset will shut down the operating system.
4. If the error remains after the system-management processor is reset, reset the primary CMM.

No hardware components have to be replaced.

- **35010844 : Unexpected exception was encountered in security service or system-management processor on [arg1].**

An internal exception occurred in the security service of the Chassis Management Module (CMM) or in the specified system-management processor. The specified node might not power on. You might not be able to log in to the system-management processor. The Flex System Manager management software might not be able to communicate with the system-management processor. Support will address this software issue and must engage Product Engineering, who will engage Development. CMM and node service data is required.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0406

User Response
Complete the following steps as a workaround until the problem is solved:

1. Make sure that the CMM and the affected node have the correct level of firmware.
2. Check the firmware change history for security updates.
3. To manually retry the operation, reset the affected system-management processor on the node. If you cannot reset the system-management processor from the Flex System Manager management software, reset it from the CMM. If you have problems resetting the affected system-management processor, perform a service-level reset of the node. Note that a service-level reset will shut down the operating system.
4. If the error remains after the system-management processor is reset, reset the primary CMM.

No hardware components have to be replaced.

- **35010845 : Unexpected exception was encountered in security service or system-management processor on [arg1].**

  An internal exception occurred in the security service of the Chassis Management Module (CMM) or in the specified system-management processor. The specified node might not power on. You might not be able to log in to the system-management processor. The Flex System Manager management software might not be able to communicate with the system-management processor. Support will address this software issue and must engage Product Engineering, who will engage Development. CMM and node service data is required.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Nodes (Critical)

  SNMP Trap ID
  mmTrapBladeC

  CIM Information
  Prefix: CMM **ID:** 0406

  User Response
  Complete the following steps as a workaround until the problem is solved:

  1. Make sure that the CMM and the affected node have the correct level of firmware.
  2. Check the firmware change history for security updates.
  3. To manually retry the operation, reset the affected system-management processor on the node. If you cannot reset the system-management processor from the Flex System Manager management software, reset it from the CMM. If you have problems resetting the affected system-management processor, perform a service-level reset of the node. Note that a service-level reset will shut down the operating system.
  4. If the error remains after the system-management processor is reset, reset the primary CMM.

  No hardware components have to be replaced.

- **35010846 : Unexpected exception was encountered in security service or system-management processor on [arg1].**

  An internal exception occurred in the security service of the Chassis Management Module (CMM) or in the specified system-management processor. The specified node might not power on. You might not be able to log in to the system-management processor. The Flex System Manager management software might not be able to communicate with the system-management processor. Support will address this software

issue and must engage Product Engineering, who will engage Development. CMM and node service data is required.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0406

User Response
Complete the following steps as a workaround until the problem is solved:

1. Make sure that the CMM and the affected node have the correct level of firmware.
2. Check the firmware change history for security updates.
3. To manually retry the operation, reset the affected system-management processor on the node. If you cannot reset the system-management processor from the Flex System Manager management software, reset it from the CMM. If you have problems resetting the affected system-management processor, perform a service-level reset of the node. Note that a service-level reset will shut down the operating system.
4. If the error remains after the system-management processor is reset, reset the primary CMM.

No hardware components have to be replaced.

- **35010847 : Unexpected exception was encountered in security service or system-management processor on [arg1].**

An internal exception occurred in the security service of the Chassis Management Module (CMM) or in the specified system-management processor. The specified node might not power on. You might not be able to log in to the system-management processor. The Flex System Manager management software might not be able to communicate with the system-management processor. Support will address this software issue and must engage Product Engineering, who will engage Development. CMM and node service data is required.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0406

User Response

Complete the following steps as a workaround until the problem is solved:

1. Make sure that the CMM and the affected node have the correct level of firmware.
2. Check the firmware change history for security updates.
3. To manually retry the operation, reset the affected system-management processor on the node. If you cannot reset the system-management processor from the Flex System Manager management software, reset it from the CMM. If you have problems resetting the affected system-management processor, perform a service-level reset of the node. Note that a service-level reset will shut down the operating system.
4. If the error remains after the system-management processor is reset, reset the primary CMM.

No hardware components have to be replaced.

- **35010848 : Unexpected exception was encountered in security service or system-management processor on [arg1].**

  An internal exception occurred in the security service of the Chassis Management Module (CMM) or in the specified system-management processor. The specified node might not power on. You might not be able to log in to the system-management processor. The Flex System Manager management software might not be able to communicate with the system-management processor. Support will address this software issue and must engage Product Engineering, who will engage Development. CMM and node service data is required.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Nodes (Critical)

  SNMP Trap ID
  mmTrapBladeC

  CIM Information
  Prefix: CMM **ID:** 0406

  User Response

  Complete the following steps as a workaround until the problem is solved:

  1. Make sure that the CMM and the affected node have the correct level of firmware.
  2. Check the firmware change history for security updates.
  3. To manually retry the operation, reset the affected system-management processor on the node. If you cannot reset the system-management processor from the Flex System Manager management software, reset it from the CMM. If you have problems resetting the affected system-management processor, perform a service-level reset of the node. Note that a service-level reset will shut down the operating system.
  4. If the error remains after the system-management processor is reset, reset the primary CMM.

  No hardware components have to be replaced.

- **35010849 : Unexpected exception was encountered in security service or system-management processor on [arg1].**

  An internal exception occurred in the security service of the Chassis Management Module (CMM) or in the specified system-management processor. The specified node might not power on. You might not be able

to log in to the system-management processor. The Flex System Manager management software might not be able to communicate with the system-management processor. Support will address this software issue and must engage Product Engineering, who will engage Development. CMM and node service data is required.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0406

User Response
Complete the following steps as a workaround until the problem is solved:

1. Make sure that the CMM and the affected node have the correct level of firmware.
2. Check the firmware change history for security updates.
3. To manually retry the operation, reset the affected system-management processor on the node. If you cannot reset the system-management processor from the Flex System Manager management software, reset it from the CMM. If you have problems resetting the affected system-management processor, perform a service-level reset of the node. Note that a service-level reset will shut down the operating system.
4. If the error remains after the system-management processor is reset, reset the primary CMM.

No hardware components have to be replaced.

- **3501084A : Unexpected exception was encountered in security service or system-management processor on [arg1].**

An internal exception occurred in the security service of the Chassis Management Module (CMM) or in the specified system-management processor. The specified node might not power on. You might not be able to log in to the system-management processor. The Flex System Manager management software might not be able to communicate with the system-management processor. Support will address this software issue and must engage Product Engineering, who will engage Development. CMM and node service data is required.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0406

User Response
Complete the following steps as a workaround until the problem is solved:

1. Make sure that the CMM and the affected node have the correct level of firmware.
2. Check the firmware change history for security updates.
3. To manually retry the operation, reset the affected system-management processor on the node. If you cannot reset the system-management processor from the Flex System Manager management software, reset it from the CMM. If you have problems resetting the affected system-management processor, perform a service-level reset of the node. Note that a service-level reset will shut down the operating system.
4. If the error remains after the system-management processor is reset, reset the primary CMM.

No hardware components have to be replaced.

- **3501084B : Unexpected exception was encountered in security service or system-management processor on [arg1].**

An internal exception occurred in the security service of the Chassis Management Module (CMM) or in the specified system-management processor. The specified node might not power on. You might not be able to log in to the system-management processor. The Flex System Manager management software might not be able to communicate with the system-management processor. Support will address this software issue and must engage Product Engineering, who will engage Development. CMM and node service data is required.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0406

User Response
Complete the following steps as a workaround until the problem is solved:

1. Make sure that the CMM and the affected node have the correct level of firmware.
2. Check the firmware change history for security updates.
3. To manually retry the operation, reset the affected system-management processor on the node. If you cannot reset the system-management processor from the Flex System Manager management software, reset it from the CMM. If you have problems resetting the affected system-management processor, perform a service-level reset of the node. Note that a service-level reset will shut down the operating system.
4. If the error remains after the system-management processor is reset, reset the primary CMM.

No hardware components have to be replaced.

- **3501084C : Unexpected exception was encountered in security service or system-management processor on [arg1].**

An internal exception occurred in the security service of the Chassis Management Module (CMM) or in the specified system-management processor. The specified node might not power on. You might not be able to log in to the system-management processor. The Flex System Manager management software might not be able to communicate with the system-management processor. Support will address this software issue and must engage Product Engineering, who will engage Development. CMM and node service data is required.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0406

User Response
Complete the following steps as a workaround until the problem is solved:

1. Make sure that the CMM and the affected node have the correct level of firmware.
2. Check the firmware change history for security updates.
3. To manually retry the operation, reset the affected system-management processor on the node. If you cannot reset the system-management processor from the Flex System Manager management software, reset it from the CMM. If you have problems resetting the affected system-management processor, perform a service-level reset of the node. Note that a service-level reset will shut down the operating system.
4. If the error remains after the system-management processor is reset, reset the primary CMM.

No hardware components have to be replaced.

- **3501084D : Unexpected exception was encountered in security service or system-management processor on [arg1].**

An internal exception occurred in the security service of the Chassis Management Module (CMM) or in the specified system-management processor. The specified node might not power on. You might not be able to log in to the system-management processor. The Flex System Manager management software might not be able to communicate with the system-management processor. Support will address this software issue and must engage Product Engineering, who will engage Development. CMM and node service data is required.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0406

User Response
Complete the following steps as a workaround until the problem is solved:

1. Make sure that the CMM and the affected node have the correct level of firmware.
2. Check the firmware change history for security updates.
3. To manually retry the operation, reset the affected system-management processor on the node. If you cannot reset the system-management processor from the Flex System Manager management software, reset it from the CMM. If you have problems resetting the affected system-management processor, perform a service-level reset of the node. Note that a service-level reset will shut down the operating system.
4. If the error remains after the system-management processor is reset, reset the primary CMM.

No hardware components have to be replaced.

- **3501084E : Unexpected exception was encountered in security service or system-management processor on [arg1].**

An internal exception occurred in the security service of the Chassis Management Module (CMM) or in the specified system-management processor. The specified node might not power on. You might not be able to log in to the system-management processor. The Flex System Manager management software might not be able to communicate with the system-management processor. Support will address this software issue and must engage Product Engineering, who will engage Development. CMM and node service data is required.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0406

User Response
Complete the following steps as a workaround until the problem is solved:

1. Make sure that the CMM and the affected node have the correct level of firmware.
2. Check the firmware change history for security updates.
3. To manually retry the operation, reset the affected system-management processor on the node. If you cannot reset the system-management processor from the Flex System Manager management software, reset it from the CMM. If you have problems resetting the affected system-management processor, perform a service-level reset of the node. Note that a service-level reset will shut down the operating system.
4. If the error remains after the system-management processor is reset, reset the primary CMM.

No hardware components have to be replaced.

- **35010881 : The system-management processor on [arg1] was reset by the Chassis Management Module for the security service.**

  The Chassis Management Module has reset the system-management processor in the specified node one or more times because the security service had to establish communication with the system-management processor.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0408

  User Response
  Information only; no action is required.
- **35010882 : The system-management processor on [arg1] was reset by the Chassis Management Module for the security service.**

  The Chassis Management Module has reset the system-management processor in the specified node one or more times because the security service had to establish communication with the system-management processor.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0408

  User Response
  Information only; no action is required.
- **35010883 : The system-management processor on [arg1] was reset by the Chassis Management Module for the security service.**

  The Chassis Management Module has reset the system-management processor in the specified node one or more times because the security service had to establish communication with the system-management processor.

  Severity

Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0408

User Response
Information only; no action is required.

- **35010884 : The system-management processor on [arg1] was reset by the Chassis Management Module for the security service.**

  The Chassis Management Module has reset the system-management processor in the specified node one or more times because the security service had to establish communication with the system-management processor.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0408

  User Response
  Information only; no action is required.

- **35010885 : The system-management processor on [arg1] was reset by the Chassis Management Module for the security service.**

  The Chassis Management Module has reset the system-management processor in the specified node one or more times because the security service had to establish communication with the system-management processor.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category

Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0408

User Response
Information only; no action is required.

- **35010886 : The system-management processor on [arg1] was reset by the Chassis Management Module for the security service.**

  The Chassis Management Module has reset the system-management processor in the specified node one or more times because the security service had to establish communication with the system-management processor.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0408

  User Response
  Information only; no action is required.

- **35010887 : The system-management processor on [arg1] was reset by the Chassis Management Module for the security service.**

  The Chassis Management Module has reset the system-management processor in the specified node one or more times because the security service had to establish communication with the system-management processor.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0408

  User Response

Information only; no action is required.

- **35010888 : The system-management processor on [arg1] was reset by the Chassis Management Module for the security service.**

  The Chassis Management Module has reset the system-management processor in the specified node one or more times because the security service had to establish communication with the system-management processor.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0408

  User Response
  Information only; no action is required.

- **35010889 : The system-management processor on [arg1] was reset by the Chassis Management Module for the security service.**

  The Chassis Management Module has reset the system-management processor in the specified node one or more times because the security service had to establish communication with the system-management processor.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0408

  User Response
  Information only; no action is required.

- **3501088A : The system-management processor on [arg1] was reset by the Chassis Management Module for the security service.**

  The Chassis Management Module has reset the system-management processor in the specified node one or more times because the security service had to establish communication with the system-management processor.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0408

User Response
Information only; no action is required.

- **3501088B : The system-management processor on [arg1] was reset by the Chassis Management Module for the security service.**

  The Chassis Management Module has reset the system-management processor in the specified node one or more times because the security service had to establish communication with the system-management processor.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0408

  User Response
  Information only; no action is required.

- **3501088C : The system-management processor on [arg1] was reset by the Chassis Management Module for the security service.**

  The Chassis Management Module has reset the system-management processor in the specified node one or more times because the security service had to establish communication with the system-management processor.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0408

User Response
Information only; no action is required.

- **3501088D : The system-management processor on [arg1] was reset by the Chassis Management Module for the security service.**

  The Chassis Management Module has reset the system-management processor in the specified node one or more times because the security service had to establish communication with the system-management processor.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0408

  User Response
  Information only; no action is required.

- **3501088E : The system-management processor on [arg1] was reset by the Chassis Management Module for the security service.**

  The Chassis Management Module has reset the system-management processor in the specified node one or more times because the security service had to establish communication with the system-management processor.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0408

User Response
Information only; no action is required.

- **35010900 : The Chassis Management Module security service encountered a recoverable error.**

  The Chassis Management Module security service has automatically recovered from a recoverable error condition. The automatic recovery steps may have resulted in secondary effects, such as the provisioning of new trust certificates or the resetting of the system-management processors for one or more nodes in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0771

  User Response
  Information only; no action is required.

- **35010A00 : Chassis Management Module configuration is not compliant with the security policy.**

  An internal exception occurred in the security service of the Chassis Management Module (CMM). The current security policy level requires that some network protocols to be disabled or other CMM configurations to be compliant with the security policy level.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0870

  User Response
  Please go to Mgt Module Management -> Security -> Security Policies for further details how to become compliant.

- **35010B01 : System-management processor firmware on [arg1] does not support the certificate cryptography algorithm configured on the CMM.**

  The system-management processor for the specified node does not support the certificate cryptography algorithm configured at the management module. The service processor may not be able to utilize the

certificates it has been provisioned with. System-management functions may not work correctly, including web interface and user login.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0753

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the certificate cryptography algorithm to the "RSA2048-SHA1" setting on the CMM

- **35010B02 : System-management processor firmware on [arg1] does not support the certificate cryptography algorithm configured on the CMM.**

  The system-management processor for the specified node does not support the certificate cryptography algorithm configured at the management module. The service processor may not be able to utilize the certificates it has been provisioned with. System-management functions may not work correctly, including web interface and user login.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0753

  User Response
  Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the certificate cryptography algorithm to the "RSA2048-SHA1" setting on the CMM

- **35010B03 : System-management processor firmware on [arg1] does not support the certificate cryptography algorithm configured on the CMM.**

  The system-management processor for the specified node does not support the certificate cryptography algorithm configured at the management module. The service processor may not be able to utilize the

certificates it has been provisioned with. System-management functions may not work correctly, including web interface and user login.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0753

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the certificate cryptography algorithm to the "RSA2048-SHA1" setting on the CMM

- **35010B04 : System-management processor firmware on [arg1] does not support the certificate cryptography algorithm configured on the CMM.**

  The system-management processor for the specified node does not support the certificate cryptography algorithm configured at the management module. The service processor may not be able to utilize the certificates it has been provisioned with. System-management functions may not work correctly, including web interface and user login.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0753

  User Response
  Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the certificate cryptography algorithm to the "RSA2048-SHA1" setting on the CMM

- **35010B05 : System-management processor firmware on [arg1] does not support the certificate cryptography algorithm configured on the CMM.**

  The system-management processor for the specified node does not support the certificate cryptography algorithm configured at the management module. The service processor may not be able to utilize the

certificates it has been provisioned with. System-management functions may not work correctly, including web interface and user login.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0753

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the certificate cryptography algorithm to the "RSA2048-SHA1" setting on the CMM

- **35010B06 : System-management processor firmware on [arg1] does not support the certificate cryptography algorithm configured on the CMM.**

  The system-management processor for the specified node does not support the certificate cryptography algorithm configured at the management module. The service processor may not be able to utilize the certificates it has been provisioned with. System-management functions may not work correctly, including web interface and user login.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0753

  User Response
  Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the certificate cryptography algorithm to the "RSA2048-SHA1" setting on the CMM

- **35010B07 : System-management processor firmware on [arg1] does not support the certificate cryptography algorithm configured on the CMM.**

  The system-management processor for the specified node does not support the certificate cryptography algorithm configured at the management module. The service processor may not be able to utilize the

certificates it has been provisioned with. System-management functions may not work correctly, including web interface and user login.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0753

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the certificate cryptography algorithm to the "RSA2048-SHA1" setting on the CMM

- **35010B08 : System-management processor firmware on [arg1] does not support the certificate cryptography algorithm configured on the CMM.**

  The system-management processor for the specified node does not support the certificate cryptography algorithm configured at the management module. The service processor may not be able to utilize the certificates it has been provisioned with. System-management functions may not work correctly, including web interface and user login.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0753

  User Response
  Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the certificate cryptography algorithm to the "RSA2048-SHA1" setting on the CMM

- **35010B09 : System-management processor firmware on [arg1] does not support the certificate cryptography algorithm configured on the CMM.**

  The system-management processor for the specified node does not support the certificate cryptography algorithm configured at the management module. The service processor may not be able to utilize the

certificates it has been provisioned with. System-management functions may not work correctly, including web interface and user login.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0753

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the certificate cryptography algorithm to the "RSA2048-SHA1" setting on the CMM

- **35010B0A : System-management processor firmware on [arg1] does not support the certificate cryptography algorithm configured on the CMM.**

  The system-management processor for the specified node does not support the certificate cryptography algorithm configured at the management module. The service processor may not be able to utilize the certificates it has been provisioned with. System-management functions may not work correctly, including web interface and user login.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0753

  User Response
  Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the certificate cryptography algorithm to the "RSA2048-SHA1" setting on the CMM

- **35010B0B : System-management processor firmware on [arg1] does not support the certificate cryptography algorithm configured on the CMM.**

  The system-management processor for the specified node does not support the certificate cryptography algorithm configured at the management module. The service processor may not be able to utilize the

certificates it has been provisioned with. System-management functions may not work correctly, including web interface and user login.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0753

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the certificate cryptography algorithm to the "RSA2048-SHA1" setting on the CMM

- **35010B0C : System-management processor firmware on [arg1] does not support the certificate cryptography algorithm configured on the CMM.**

  The system-management processor for the specified node does not support the certificate cryptography algorithm configured at the management module. The service processor may not be able to utilize the certificates it has been provisioned with. System-management functions may not work correctly, including web interface and user login.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0753

  User Response
  Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the certificate cryptography algorithm to the "RSA2048-SHA1" setting on the CMM

- **35010B0D : System-management processor firmware on [arg1] does not support the certificate cryptography algorithm configured on the CMM.**

  The system-management processor for the specified node does not support the certificate cryptography algorithm configured at the management module. The service processor may not be able to utilize the

certificates it has been provisioned with. System-management functions may not work correctly, including web interface and user login.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0753

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the certificate cryptography algorithm to the "RSA2048-SHA1" setting on the CMM

- **35010B0E : System-management processor firmware on [arg1] does not support the certificate cryptography algorithm configured on the CMM.**

  The system-management processor for the specified node does not support the certificate cryptography algorithm configured at the management module. The service processor may not be able to utilize the certificates it has been provisioned with. System-management functions may not work correctly, including web interface and user login.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0753

  User Response
  Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the certificate cryptography algorithm to the "RSA2048-SHA1" setting on the CMM

- **35010C01 : System-management processor firmware on [arg1] does not support Authentication Only mode.**

Authentication Only mode enabled on the Chassis Management Module is not supported by the system-management processor for the specified node. Users might not be able to log into the node system-management processor.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0590

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily disable Authentication Only mode on the CMM.

- **35010C02 : System-management processor firmware on [arg1] does not support Authentication Only mode.**

Authentication Only mode enabled on the Chassis Management Module is not supported by the system-management processor for the specified node. Users might not be able to log into the node system-management processor.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0590

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily disable Authentication Only mode on the CMM.

- **35010C03 : System-management processor firmware on [arg1] does not support Authentication Only mode.**

Authentication Only mode enabled on the Chassis Management Module is not supported by the system-management processor for the specified node. Users might not be able to log into the node system-management processor.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0590

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily disable Authentication Only mode on the CMM.

- **35010C04 : System-management processor firmware on [arg1] does not support Authentication Only mode.**

Authentication Only mode enabled on the Chassis Management Module is not supported by the system-management processor for the specified node. Users might not be able to log into the node system-management processor.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0590

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily disable Authentication Only mode on the CMM.

- **35010C05 : System-management processor firmware on [arg1] does not support Authentication Only mode.**

Authentication Only mode enabled on the Chassis Management Module is not supported by the system-management processor for the specified node. Users might not be able to log into the node system-management processor.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0590

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily disable Authentication Only mode on the CMM.

- **35010C06 : System-management processor firmware on [arg1] does not support Authentication Only mode.**

Authentication Only mode enabled on the Chassis Management Module is not supported by the system-management processor for the specified node. Users might not be able to log into the node system-management processor.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0590

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily disable Authentication Only mode on the CMM.

- **35010C07 : System-management processor firmware on [arg1] does not support Authentication Only mode.**

Authentication Only mode enabled on the Chassis Management Module is not supported by the system-management processor for the specified node. Users might not be able to log into the node system-management processor.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0590

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily disable Authentication Only mode on the CMM.

- **35010C08 : System-management processor firmware on [arg1] does not support Authentication Only mode.**

Authentication Only mode enabled on the Chassis Management Module is not supported by the system-management processor for the specified node. Users might not be able to log into the node system-management processor.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0590

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily disable Authentication Only mode on the CMM.

- **35010C09 : System-management processor firmware on [arg1] does not support Authentication Only mode.**

Authentication Only mode enabled on the Chassis Management Module is not supported by the system-management processor for the specified node. Users might not be able to log into the node system-management processor.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0590

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily disable Authentication Only mode on the CMM.

- **35010C0A : System-management processor firmware on [arg1] does not support Authentication Only mode.**

Authentication Only mode enabled on the Chassis Management Module is not supported by the system-management processor for the specified node. Users might not be able to log into the node system-management processor.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0590

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily disable Authentication Only mode on the CMM.

- **35010C0B : System-management processor firmware on [arg1] does not support Authentication Only mode.**

Authentication Only mode enabled on the Chassis Management Module is not supported by the system-management processor for the specified node. Users might not be able to log into the node system-management processor.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0590

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily disable Authentication Only mode on the CMM.

- **35010C0C : System-management processor firmware on [arg1] does not support Authentication Only mode.**

  Authentication Only mode enabled on the Chassis Management Module is not supported by the system-management processor for the specified node. Users might not be able to log into the node system-management processor.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0590

  User Response
  Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily disable Authentication Only mode on the CMM.

- **35010C0D : System-management processor firmware on [arg1] does not support Authentication Only mode.**

Authentication Only mode enabled on the Chassis Management Module is not supported by the system-management processor for the specified node. Users might not be able to log into the node system-management processor.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0590

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily disable Authentication Only mode on the CMM.

- **35010C0E : System-management processor firmware on [arg1] does not support Authentication Only mode.**

Authentication Only mode enabled on the Chassis Management Module is not supported by the system-management processor for the specified node. Users might not be able to log into the node system-management processor.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0590

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily disable Authentication Only mode on the CMM.

- **35010D01 : System-management processor firmware on [arg1] does not support the cryptography mode configured on the CMM.**

The system-management processor for the specified node does not support the cryptography mode configured at the management module. System-management functions may not work correctly, including web interface and user login

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0751

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the cryptography mode to the "compatible" setting on the CMM, until all of the node system-management processor's in the chassis can support the desired cryptography mode.

- **35010D02 : System-management processor firmware on [arg1] does not support the cryptography mode configured on the CMM.**

The system-management processor for the specified node does not support the cryptography mode configured at the management module. System-management functions may not work correctly, including web interface and user login

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0751

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the cryptography mode to the "compatible" setting on the CMM, until all of the node system-management processor's in the chassis can support the desired cryptography mode.

- **35010D03 : System-management processor firmware on [arg1] does not support the cryptography mode configured on the CMM.**

The system-management processor for the specified node does not support the cryptography mode configured at the management module. System-management functions may not work correctly, including web interface and user login

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0751

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the cryptography mode to the "compatible" setting on the CMM, until all of the node system-management processor's in the chassis can support the desired cryptography mode.

- **35010D04 : System-management processor firmware on [arg1] does not support the cryptography mode configured on the CMM.**

The system-management processor for the specified node does not support the cryptography mode configured at the management module. System-management functions may not work correctly, including web interface and user login

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0751

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the cryptography mode to the "compatible" setting on the CMM, until all of the node system-management processor's in the chassis can support the desired cryptography mode.

- **35010D05 : System-management processor firmware on [arg1] does not support the cryptography mode configured on the CMM.**

The system-management processor for the specified node does not support the cryptography mode configured at the management module. System-management functions may not work correctly, including web interface and user login

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0751

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the cryptography mode to the "compatible" setting on the CMM, until all of the node system-management processor's in the chassis can support the desired cryptography mode.

- **35010D06 : System-management processor firmware on [arg1] does not support the cryptography mode configured on the CMM.**

The system-management processor for the specified node does not support the cryptography mode configured at the management module. System-management functions may not work correctly, including web interface and user login

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0751

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the cryptography mode to the "compatible" setting on the CMM, until all of the node system-management processor's in the chassis can support the desired cryptography mode.

- **35010D07 : System-management processor firmware on [arg1] does not support the cryptography mode configured on the CMM.**

The system-management processor for the specified node does not support the cryptography mode configured at the management module. System-management functions may not work correctly, including web interface and user login

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0751

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the cryptography mode to the "compatible" setting on the CMM, until all of the node system-management processor's in the chassis can support the desired cryptography mode.

- **35010D08 : System-management processor firmware on [arg1] does not support the cryptography mode configured on the CMM.**

The system-management processor for the specified node does not support the cryptography mode configured at the management module. System-management functions may not work correctly, including web interface and user login

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0751

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the cryptography mode to the "compatible" setting on the CMM, until all of the node system-management processor's in the chassis can support the desired cryptography mode.

- **35010D09 : System-management processor firmware on [arg1] does not support the cryptography mode configured on the CMM.**

The system-management processor for the specified node does not support the cryptography mode configured at the management module. System-management functions may not work correctly, including web interface and user login

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0751

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the cryptography mode to the "compatible" setting on the CMM, until all of the node system-management processor's in the chassis can support the desired cryptography mode.

- **35010D0A : System-management processor firmware on [arg1] does not support the cryptography mode configured on the CMM.**

The system-management processor for the specified node does not support the cryptography mode configured at the management module. System-management functions may not work correctly, including web interface and user login

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0751

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the cryptography mode to the "compatible" setting on the CMM, until all of the node system-management processor's in the chassis can support the desired cryptography mode.

- **35010D0B : System-management processor firmware on [arg1] does not support the cryptography mode configured on the CMM.**

The system-management processor for the specified node does not support the cryptography mode configured at the management module. System-management functions may not work correctly, including web interface and user login

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0751

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the cryptography mode to the "compatible" setting on the CMM, until all of the node system-management processor's in the chassis can support the desired cryptography mode.

- **35010D0C : System-management processor firmware on [arg1] does not support the cryptography mode configured on the CMM.**

The system-management processor for the specified node does not support the cryptography mode configured at the management module. System-management functions may not work correctly, including web interface and user login

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0751

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the cryptography mode to the "compatible" setting on the CMM, until all of the node system-management processor's in the chassis can support the desired cryptography mode.

- **35010D0D : System-management processor firmware on [arg1] does not support the cryptography mode configured on the CMM.**

The system-management processor for the specified node does not support the cryptography mode configured at the management module. System-management functions may not work correctly, including web interface and user login

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0751

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the cryptography mode to the "compatible" setting on the CMM, until all of the node system-management processor's in the chassis can support the desired cryptography mode.

- **35010D0E : System-management processor firmware on [arg1] does not support the cryptography mode configured on the CMM.**

The system-management processor for the specified node does not support the cryptography mode configured at the management module. System-management functions may not work correctly, including web interface and user login

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0751

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the cryptography mode to the "compatible" setting on the CMM, until all of the node system-management processor's in the chassis can support the desired cryptography mode.

- **35010E01 : System-management processor firmware on [arg1] does not support the cipher suite level selected on the Chassis Management Module.**

The system-management processor for the specified node does not support the setting of the cipher suite level that was selected on the Chassis Management Module. The system-management processor's web server might allow connections using cipher suites below the desired minimum level. Also, users might not be able to log into the node system-management processor.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0716

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the cipher suite level to the "legacy" setting on the CMM.

- **35010E02 : System-management processor firmware on [arg1] does not support the cipher suite level selected on the Chassis Management Module.**

  The system-management processor for the specified node does not support the setting of the cipher suite level that was selected on the Chassis Management Module. The system-management processor's web server might allow connections using cipher suites below the desired minimum level. Also, users might not be able to log into the node system-management processor.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0716

  User Response
  Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the cipher suite level to the "legacy" setting on the CMM.

- **35010E03 : System-management processor firmware on [arg1] does not support the cipher suite level selected on the Chassis Management Module.**

The system-management processor for the specified node does not support the setting of the cipher suite level that was selected on the Chassis Management Module. The system-management processor's web server might allow connections using cipher suites below the desired minimum level. Also, users might not be able to log into the node system-management processor.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0716

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the cipher suite level to the "legacy" setting on the CMM.

- **35010E04 : System-management processor firmware on [arg1] does not support the cipher suite level selected on the Chassis Management Module.**

The system-management processor for the specified node does not support the setting of the cipher suite level that was selected on the Chassis Management Module. The system-management processor's web server might allow connections using cipher suites below the desired minimum level. Also, users might not be able to log into the node system-management processor.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0716

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the cipher suite level to the "legacy" setting on the CMM.

- **35010E05 : System-management processor firmware on [arg1] does not support the cipher suite level selected on the Chassis Management Module.**

The system-management processor for the specified node does not support the setting of the cipher suite level that was selected on the Chassis Management Module. The system-management processor's web server might allow connections using cipher suites below the desired minimum level. Also, users might not be able to log into the node system-management processor.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0716

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the cipher suite level to the "legacy" setting on the CMM.

- **35010E06 : System-management processor firmware on [arg1] does not support the cipher suite level selected on the Chassis Management Module.**

  The system-management processor for the specified node does not support the setting of the cipher suite level that was selected on the Chassis Management Module. The system-management processor's web server might allow connections using cipher suites below the desired minimum level. Also, users might not be able to log into the node system-management processor.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0716

  User Response
  Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the cipher suite level to the "legacy" setting on the CMM.

- **35010E07 : System-management processor firmware on [arg1] does not support the cipher suite level selected on the Chassis Management Module.**

The system-management processor for the specified node does not support the setting of the cipher suite level that was selected on the Chassis Management Module. The system-management processor's web server might allow connections using cipher suites below the desired minimum level. Also, users might not be able to log into the node system-management processor.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0716

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the cipher suite level to the "legacy" setting on the CMM.

- **35010E08 : System-management processor firmware on [arg1] does not support the cipher suite level selected on the Chassis Management Module.**

The system-management processor for the specified node does not support the setting of the cipher suite level that was selected on the Chassis Management Module. The system-management processor's web server might allow connections using cipher suites below the desired minimum level. Also, users might not be able to log into the node system-management processor.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0716

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the cipher suite level to the "legacy" setting on the CMM.

- **35010E09 : System-management processor firmware on [arg1] does not support the cipher suite level selected on the Chassis Management Module.**

The system-management processor for the specified node does not support the setting of the cipher suite level that was selected on the Chassis Management Module. The system-management processor's web server might allow connections using cipher suites below the desired minimum level. Also, users might not be able to log into the node system-management processor.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0716

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the cipher suite level to the "legacy" setting on the CMM.

- **35010E0A : System-management processor firmware on [arg1] does not support the cipher suite level selected on the Chassis Management Module.**

  The system-management processor for the specified node does not support the setting of the cipher suite level that was selected on the Chassis Management Module. The system-management processor's web server might allow connections using cipher suites below the desired minimum level. Also, users might not be able to log into the node system-management processor.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0716

  User Response
  Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the cipher suite level to the "legacy" setting on the CMM.

- **35010E0B : System-management processor firmware on [arg1] does not support the cipher suite level selected on the Chassis Management Module.**

The system-management processor for the specified node does not support the setting of the cipher suite level that was selected on the Chassis Management Module. The system-management processor's web server might allow connections using cipher suites below the desired minimum level. Also, users might not be able to log into the node system-management processor.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0716

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the cipher suite level to the "legacy" setting on the CMM.

- **35010E0C : System-management processor firmware on [arg1] does not support the cipher suite level selected on the Chassis Management Module.**

  The system-management processor for the specified node does not support the setting of the cipher suite level that was selected on the Chassis Management Module. The system-management processor's web server might allow connections using cipher suites below the desired minimum level. Also, users might not be able to log into the node system-management processor.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0716

  User Response
  Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the cipher suite level to the "legacy" setting on the CMM.

- **35010E0D : System-management processor firmware on [arg1] does not support the cipher suite level selected on the Chassis Management Module.**

The system-management processor for the specified node does not support the setting of the cipher suite level that was selected on the Chassis Management Module. The system-management processor's web server might allow connections using cipher suites below the desired minimum level. Also, users might not be able to log into the node system-management processor.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0716

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the cipher suite level to the "legacy" setting on the CMM.

- **35010E0E : System-management processor firmware on [arg1] does not support the cipher suite level selected on the Chassis Management Module.**

  The system-management processor for the specified node does not support the setting of the cipher suite level that was selected on the Chassis Management Module. The system-management processor's web server might allow connections using cipher suites below the desired minimum level. Also, users might not be able to log into the node system-management processor.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0716

  User Response
  Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the Chassis Management Module. If you cannot log onto the node system-management processor, you might need to temporarily set the cipher suite level to the "legacy" setting on the CMM.

- **35010F01 : System-management processor firmware on node [arg1] does not support the use of imported certificates for local authentication.**

The system-management processor firmware level for the specified node does not support the use of imported SSL server certificates. The Chassis Management Module (CMM) is configured to use imported an SSL server certificate, and the system-management processor for the specified node does not support that configuration. System-management functions may not work correctly, including user login to the system-management processor on the node. Note: for back-up purposes, the local authentication server on the CMM is always active, even though an external LDAP server may be used.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0796

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the CMM. If you cannot log onto the node system-management processor, you might need to temporarily configure the CMM to use a server certificate that is signed by the local CMM certificate authority (CA). Perform one of the following actions:

- Use the local CMM CA:
  1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
  2. Select the option for the local-internally signed SSL Server Certificate.
- Attempt to reapply the installed certificate:
  1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
  2. Select Re-Apply Installed Certificate. Not all nodes in the chassis can support the use of imported SSL certificate, this option will result in the LDAP server using a SSL certificate signed by the local CMM CA. The CMM will begin using the imported certificate for the local authentication server after the system-management processor firmware levels for all nodes in the chassis have been updated, and the imported server certificate is re-applied using again the "Re-Apply Installed Certificate" option.

- **35010F02 : System-management processor firmware on node [arg1] does not support the use of imported certificates for local authentication.**

The system-management processor firmware level for the specified node does not support the use of imported SSL server certificates. The Chassis Management Module (CMM) is configured to use imported an SSL server certificate, and the system-management processor for the specified node does not support that configuration. System-management functions may not work correctly, including user login to the system-management processor on the node. Note: for back-up purposes, the local authentication server on the CMM is always active, even though an external LDAP server may be used.

Severity
Warning

Serviceable

Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0796

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the CMM. If you cannot log onto the node system-management processor, you might need to temporarily configure the CMM to use a server certificate that is signed by the local CMM certificate authority (CA). Perform one of the following actions:

- Use the local CMM CA:
  1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
  2. Select the option for the local-internally signed SSL Server Certificate.
- Attempt to reapply the installed certificate:
  1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
  2. Select Re-Apply Installed Certificate. Not all nodes in the chassis can support the use of imported SSL certificate, this option will result in the LDAP server using a SSL certificate signed by the local CMM CA. The CMM will begin using the imported certificate for the local authentication server after the system-management processor firmware levels for all nodes in the chassis have been updated, and the imported server certificate is re-applied using again the "Re-Apply Installed Certificate" option.

- **35010F03 : System-management processor firmware on node [arg1] does not support the use of imported certificates for local authentication.**

The system-management processor firmware level for the specified node does not support the use of imported SSL server certificates. The Chassis Management Module (CMM) is configured to use imported an SSL server certificate, and the system-management processor for the specified node does not support that configuration. System-management functions may not work correctly, including user login to the system-management processor on the node. Note: for back-up purposes, the local authentication server on the CMM is always active, even though an external LDAP server may be used.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0796

User Response

Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the CMM. If you cannot log onto the node system-management processor, you might need to temporarily configure the CMM to use a server certificate that is signed by the local CMM certificate authority (CA). Perform one of the following actions:

- Use the local CMM CA:
  1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
  2. Select the option for the local-internally signed SSL Server Certificate.
- Attempt to reapply the installed certificate:
  1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
  2. Select Re-Apply Installed Certificate. Not all nodes in the chassis can support the use of imported SSL certificate, this option will result in the LDAP server using a SSL certificate signed by the local CMM CA. The CMM will begin using the imported certificate for the local authentication server after the system-management processor firmware levels for all nodes in the chassis have been updated, and the imported server certificate is re-applied using again the "Re-Apply Installed Certificate" option.

- **35010F04 : System-management processor firmware on node [arg1] does not support the use of imported certificates for local authentication.**

The system-management processor firmware level for the specified node does not support the use of imported SSL server certificates. The Chassis Management Module (CMM) is configured to use imported an SSL server certificate, and the system-management processor for the specified node does not support that configuration. System-management functions may not work correctly, including user login to the system-management processor on the node. Note: for back-up purposes, the local authentication server on the CMM is always active, even though an external LDAP server may be used.

Severity

Warning

Serviceable

Yes

Automatically notify support

No

Alert Category

Nodes (Warning)

SNMP Trap ID

mmTrapBladeN

CIM Information

Prefix: CMM **ID:** 0796

User Response

Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the CMM. If you cannot log onto the node system-management processor, you might need to temporarily configure the CMM to use a server certificate that is signed by the local CMM certificate authority (CA). Perform one of the following actions:

- Use the local CMM CA:
  1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
  2. Select the option for the local-internally signed SSL Server Certificate.
- Attempt to reapply the installed certificate:

1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
2. Select Re-Apply Installed Certificate. Not all nodes in the chassis can support the use of imported SSL certificate, this option will result in the LDAP server using a SSL certificate signed by the local CMM CA. The CMM will begin using the imported certificate for the local authentication server after the system-management processor firmware levels for all nodes in the chassis have been updated, and the imported server certificate is re-applied using again the "Re-Apply Installed Certificate" option.

- **35010F05 : System-management processor firmware on node [arg1] does not support the use of imported certificates for local authentication.**

  The system-management processor firmware level for the specified node does not support the use of imported SSL server certificates. The Chassis Management Module (CMM) is configured to use imported an SSL server certificate, and the system-management processor for the specified node does not support that configuration. System-management functions may not work correctly, including user login to the system-management processor on the node. Note: for back-up purposes, the local authentication server on the CMM is always active, even though an external LDAP server may be used.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0796

  User Response
  Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the CMM. If you cannot log onto the node system-management processor, you might need to temporarily configure the CMM to use a server certificate that is signed by the local CMM certificate authority (CA). Perform one of the following actions:
  - Use the local CMM CA:
    1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
    2. Select the option for the local-internally signed SSL Server Certificate.
  - Attempt to reapply the installed certificate:
    1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
    2. Select Re-Apply Installed Certificate. Not all nodes in the chassis can support the use of imported SSL certificate, this option will result in the LDAP server using a SSL certificate signed by the local CMM CA. The CMM will begin using the imported certificate for the local authentication server after the system-management processor firmware levels for all nodes in the chassis have been updated, and the imported server certificate is re-applied using again the "Re-Apply Installed Certificate" option.

- **35010F07 : System-management processor firmware on node [arg1] does not support the use of imported certificates for local authentication.**

The system-management processor firmware level for the specified node does not support the use of imported SSL server certificates. The Chassis Management Module (CMM) is configured to use imported an SSL server certificate, and the system-management processor for the specified node does not support that configuration. System-management functions may not work correctly, including user login to the system-management processor on the node. Note: for back-up purposes, the local authentication server on the CMM is always active, even though an external LDAP server may be used.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0796

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the CMM. If you cannot log onto the node system-management processor, you might need to temporarily configure the CMM to use a server certificate that is signed by the local CMM certificate authority (CA). Perform one of the following actions:

- Use the local CMM CA:
  1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
  2. Select the option for the local-internally signed SSL Server Certificate.
- Attempt to reapply the installed certificate:
  1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
  2. Select Re-Apply Installed Certificate. Not all nodes in the chassis can support the use of imported SSL certificate, this option will result in the LDAP server using a SSL certificate signed by the local CMM CA. The CMM will begin using the imported certificate for the local authentication server after the system-management processor firmware levels for all nodes in the chassis have been updated, and the imported server certificate is re-applied using again the "Re-Apply Installed Certificate" option.

- **35010F08 : System-management processor firmware on node [arg1] does not support the use of imported certificates for local authentication.**

The system-management processor firmware level for the specified node does not support the use of imported SSL server certificates. The Chassis Management Module (CMM) is configured to use imported an SSL server certificate, and the system-management processor for the specified node does not support that configuration. System-management functions may not work correctly, including user login to the system-management processor on the node. Note: for back-up purposes, the local authentication server on the CMM is always active, even though an external LDAP server may be used.

Severity
Warning

Serviceable

Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0796

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the CMM. If you cannot log onto the node system-management processor, you might need to temporarily configure the CMM to use a server certificate that is signed by the local CMM certificate authority (CA). Perform one of the following actions:

- Use the local CMM CA:
  1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
  2. Select the option for the local-internally signed SSL Server Certificate.
- Attempt to reapply the installed certificate:
  1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
  2. Select Re-Apply Installed Certificate. Not all nodes in the chassis can support the use of imported SSL certificate, this option will result in the LDAP server using a SSL certificate signed by the local CMM CA. The CMM will begin using the imported certificate for the local authentication server after the system-management processor firmware levels for all nodes in the chassis have been updated, and the imported server certificate is re-applied using again the "Re-Apply Installed Certificate" option.

- **35010F09 : System-management processor firmware on node [arg1] does not support the use of imported certificates for local authentication.**

The system-management processor firmware level for the specified node does not support the use of imported SSL server certificates. The Chassis Management Module (CMM) is configured to use imported an SSL server certificate, and the system-management processor for the specified node does not support that configuration. System-management functions may not work correctly, including user login to the system-management processor on the node. Note: for back-up purposes, the local authentication server on the CMM is always active, even though an external LDAP server may be used.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0796

User Response

Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the CMM. If you cannot log onto the node system-management processor, you might need to temporarily configure the CMM to use a server certificate that is signed by the local CMM certificate authority (CA). Perform one of the following actions:

- Use the local CMM CA:
  1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
  2. Select the option for the local-internally signed SSL Server Certificate.
- Attempt to reapply the installed certificate:
  1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
  2. Select Re-Apply Installed Certificate. Not all nodes in the chassis can support the use of imported SSL certificate, this option will result in the LDAP server using a SSL certificate signed by the local CMM CA. The CMM will begin using the imported certificate for the local authentication server after the system-management processor firmware levels for all nodes in the chassis have been updated, and the imported server certificate is re-applied using again the "Re-Apply Installed Certificate" option.

- **35010F0A : System-management processor firmware on node [arg1] does not support the use of imported certificates for local authentication.**

The system-management processor firmware level for the specified node does not support the use of imported SSL server certificates. The Chassis Management Module (CMM) is configured to use imported an SSL server certificate, and the system-management processor for the specified node does not support that configuration. System-management functions may not work correctly, including user login to the system-management processor on the node. Note: for back-up purposes, the local authentication server on the CMM is always active, even though an external LDAP server may be used.

Severity

Warning

Serviceable

Yes

Automatically notify support

No

Alert Category

Nodes (Warning)

SNMP Trap ID

mmTrapBladeN

CIM Information

Prefix: CMM **ID:** 0796

User Response

Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the CMM. If you cannot log onto the node system-management processor, you might need to temporarily configure the CMM to use a server certificate that is signed by the local CMM certificate authority (CA). Perform one of the following actions:

- Use the local CMM CA:
  1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
  2. Select the option for the local-internally signed SSL Server Certificate.
- Attempt to reapply the installed certificate:

1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
2. Select Re-Apply Installed Certificate. Not all nodes in the chassis can support the use of imported SSL certificate, this option will result in the LDAP server using a SSL certificate signed by the local CMM CA. The CMM will begin using the imported certificate for the local authentication server after the system-management processor firmware levels for all nodes in the chassis have been updated, and the imported server certificate is re-applied using again the "Re-Apply Installed Certificate" option.

- **35010F0B : System-management processor firmware on node [arg1] does not support the use of imported certificates for local authentication.**

  The system-management processor firmware level for the specified node does not support the use of imported SSL server certificates. The Chassis Management Module (CMM) is configured to use imported an SSL server certificate, and the system-management processor for the specified node does not support that configuration. System-management functions may not work correctly, including user login to the system-management processor on the node. Note: for back-up purposes, the local authentication server on the CMM is always active, even though an external LDAP server may be used.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Warning)

  SNMP Trap ID
  mmTrapBladeN

  CIM Information
  Prefix: CMM **ID:** 0796

  User Response
  Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the CMM. If you cannot log onto the node system-management processor, you might need to temporarily configure the CMM to use a server certificate that is signed by the local CMM certificate authority (CA). Perform one of the following actions:
  - Use the local CMM CA:
    1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
    2. Select the option for the local-internally signed SSL Server Certificate.
  - Attempt to reapply the installed certificate:
    1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
    2. Select Re-Apply Installed Certificate. Not all nodes in the chassis can support the use of imported SSL certificate, this option will result in the LDAP server using a SSL certificate signed by the local CMM CA. The CMM will begin using the imported certificate for the local authentication server after the system-management processor firmware levels for all nodes in the chassis have been updated, and the imported server certificate is re-applied using again the "Re-Apply Installed Certificate" option.

- **35010F0C : System-management processor firmware on node [arg1] does not support the use of imported certificates for local authentication.**

The system-management processor firmware level for the specified node does not support the use of imported SSL server certificates. The Chassis Management Module (CMM) is configured to use imported an SSL server certificate, and the system-management processor for the specified node does not support that configuration. System-management functions may not work correctly, including user login to the system-management processor on the node. Note: for back-up purposes, the local authentication server on the CMM is always active, even though an external LDAP server may be used.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0796

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the CMM. If you cannot log onto the node system-management processor, you might need to temporarily configure the CMM to use a server certificate that is signed by the local CMM certificate authority (CA). Perform one of the following actions:

- Use the local CMM CA:
  1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
  2. Select the option for the local-internally signed SSL Server Certificate.
- Attempt to reapply the installed certificate:
  1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
  2. Select Re-Apply Installed Certificate. Not all nodes in the chassis can support the use of imported SSL certificate, this option will result in the LDAP server using a SSL certificate signed by the local CMM CA. The CMM will begin using the imported certificate for the local authentication server after the system-management processor firmware levels for all nodes in the chassis have been updated, and the imported server certificate is re-applied using again the "Re-Apply Installed Certificate" option.

- **35010F0D : System-management processor firmware on node [arg1] does not support the use of imported certificates for local authentication.**

The system-management processor firmware level for the specified node does not support the use of imported SSL server certificates. The Chassis Management Module (CMM) is configured to use imported an SSL server certificate, and the system-management processor for the specified node does not support that configuration. System-management functions may not work correctly, including user login to the system-management processor on the node. Note: for back-up purposes, the local authentication server on the CMM is always active, even though an external LDAP server may be used.

Severity
Warning

Serviceable

Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0796

User Response
Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the CMM. If you cannot log onto the node system-management processor, you might need to temporarily configure the CMM to use a server certificate that is signed by the local CMM certificate authority (CA). Perform one of the following actions:

- Use the local CMM CA:
  1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
  2. Select the option for the local-internally signed SSL Server Certificate.
- Attempt to reapply the installed certificate:
  1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
  2. Select Re-Apply Installed Certificate. Not all nodes in the chassis can support the use of imported SSL certificate, this option will result in the LDAP server using a SSL certificate signed by the local CMM CA. The CMM will begin using the imported certificate for the local authentication server after the system-management processor firmware levels for all nodes in the chassis have been updated, and the imported server certificate is re-applied using again the "Re-Apply Installed Certificate" option.

- **35010F0E : System-management processor firmware on node [arg1] does not support the use of imported certificates for local authentication.**

The system-management processor firmware level for the specified node does not support the use of imported SSL server certificates. The Chassis Management Module (CMM) is configured to use imported an SSL server certificate, and the system-management processor for the specified node does not support that configuration. System-management functions may not work correctly, including user login to the system-management processor on the node. Note: for back-up purposes, the local authentication server on the CMM is always active, even though an external LDAP server may be used.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0796

User Response

Ensure that the node system-management processor has the correct level of firmware to support the security functions enabled on the CMM. If you cannot log onto the node system-management processor, you might need to temporarily configure the CMM to use a server certificate that is signed by the local CMM certificate authority (CA). Perform one of the following actions:

- Use the local CMM CA:
  1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
  2. Select the option for the local-internally signed SSL Server Certificate.
- Attempt to reapply the installed certificate:
  1. From the CMM web-based user interface, click Mgt Module Management->Security->SSL Server Certificate.
  2. Select Re-Apply Installed Certificate. Not all nodes in the chassis can support the use of imported SSL certificate, this option will result in the LDAP server using a SSL certificate signed by the local CMM CA. The CMM will begin using the imported certificate for the local authentication server after the system-management processor firmware levels for all nodes in the chassis have been updated, and the imported server certificate is re-applied using again the "Re-Apply Installed Certificate" option.

- **40000010 : DNS was enabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has enabled Domain Name System (DNS) on the Chassis Management Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0924

  User Response
  Information only; no action is required.

- **40000011 : DNS was disabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has disabled Domain Name System (DNS) on the Chassis Management Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID

mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0925

User Response
Information only; no action is required.

- **40000012 : The primary CMM DNS server priority setting configured as [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the Domain Name System (DNS) IPv4 and IPv6 priority configuration in the primary Chassis Management Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0144

  User Response
  Information only; no action is required.

- **40000013 : The primary CMM DNS server IP configuration was modified by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has changed the Domain Name System (DNS) IPv4 and IPv6 server address configuration in the primary Chassis Management Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0142

  User Response
  Information only; no action is required.

- **40000014 : Dynamic DNS was enabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has enabled Dynamic Domain Name System (DNS) on the Chassis Management Module.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0926

User Response
Information only; no action is required.

- **40000015 : Dynamic DNS was disabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has disabled Dynamic Domain Name System (DNS) on the Chassis Management Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0927

  User Response
  Information only; no action is required.

- **40000016 : Domain name for [arg1] CMM has been changed from [arg2] to [arg3] by user ID [arg4] from [arg5] at IP address [arg6].**

  The specified user has changed the Chassis Management Module domain name.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0525

User Response
Information only; no action is required.

- **40000017 : The standby CMM DNS server priority setting configured as [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the Domain Name System (DNS) IPv4 and IPv6 priority configuration in the standby Chassis Management Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0145

  User Response
  Information only; no action is required.

- **40000018 : The standby CMM DNS server IP configuration was modified by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has changed the Domain Name System (DNS) IPv4 and IPv6 server address configuration in the standby Chassis Management Module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0143

  User Response
  Information only; no action is required.

- **40000021 : Service data requested on node [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has requested that a service file dump be generated by a node. This log entry reports only that the request has been made, not that the operation has been completed.

  Severity

Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0280

User Response
Information only; no action is required.

- **40000022 : Node in bay [arg1] was requested to power cycle by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has requested power cycle on the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0945

  User Response
  Information only; no action is required.

- **400000F0 : Power scheduling [arg1] index = [arg2] has been [arg3] by user ID [arg4] from [arg5] at IP address [arg6].**

  The specified user has modified the power scheduling.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Power Modules (Informational)

  SNMP Trap ID
  mmTrapPowerS

CIM Information
Prefix: CMM **ID:** 0668

User Response
Information only; no action is required.

- **40000100 : Virtual reseat of node [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has performed a virtual reseat to reset the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0350

  User Response
  Information only; no action is required.

- **40000110 : Hard restart of system-management processor on [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has performed a hard restart to reset the system-management processor in the specified node.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0387

  User Response
  Information only; no action is required.

- **40001001 : License added for [arg1] type [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has added a Chassis Management Module license that allows access to the specified feature.

  Severity
  Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0388

User Response
Information only; no action is required.

- **40001002 : License removed for [arg1] type [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has removed a Chassis Management Module license from the system. Access to the specified feature is no longer allowed.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0389

  User Response
  Information only; no action is required.

- **40001003 : License serial number modified for [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the chassis serial number for a Chassis Management Module license.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0390

User Response
Information only; no action is required.

- **40001004 : License Machine Type/Model number modified for [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the machine type/model of a Chassis Management Module license.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0391

  User Response
  Information only; no action is required.

- **40001005 : License [arg1] has expired.**

  The license for the specified feature has expired. To continue using the specified feature, upgrade or renew the license.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0215

  User Response
  Information only; no action is required.

- **40001009 : Your trial license for [arg1] will expire in [arg2] days.**

  Your trial period for the specified license is about to end.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support

No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0392

User Response
Information only; no action is required.

- **40015090 : SMTP email domain changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the Simple Mail Transfer Protocol (SMTP) email domain configuration.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0584

  User Response
  Information only; no action is required.

- **4001711E : Standby Chassis Management Module failed to synchronize with the primary CMM. Standby network interface is disabled.**

  The standby Chassis Management Module (CMM) failed to synchronize with the primary CMM. The network interface for the standby CMM is disabled.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0817

  User Response
  Complete the following steps until the problem is solved:

1. Check the Chassis Management Module event log for CMM communication problems.
2. Reset the primary CMM. Do not switch over to the standby CMM.
3. Submit a service request for replacement CMMs.
4. While you wait for delivery of a replacement CMM, remove the standby CMM so that a failover cannot occur and cause settings to be lost.
5. Replace the standby CMM.
6. If replacing the standby CMM did not correct the problem, save the CMM configuration, install the replacement CMM in the primary CMM bay, and update the configuration. Return the original standby CMM to the standby CMM bay.

If the problem remains, Support will contact Product Engineering.

- **40040000 : Chassis VPD is not valid.**

  The vital product data (VPD) on the rear LED card is not valid. VPD includes information such as the serial number and part number to uniquely identify the chassis. Note that the rear LED card contains information that is needed for warranty service.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0820

  User Response
  Replace the rear LED card.

- **40040001 : Chassis VPD is not available.**

  The vital product data (VPD) on the rear LED card is not available. VPD includes information such as the serial number and part number to uniquely identify the chassis. Note that the rear LED card contains information that is needed for warranty service.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0821

User Response
Replace the rear LED card.

- **40040101 : I/O module [arg1] VPD is not valid.**

  The vital product data (VPD) of the specified I/O module is not valid. VPD includes information such as the serial number and part number to uniquely identify the I/O module.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  I/O Modules (Warning)

  SNMP Trap ID
  mmTrapION

  CIM Information
  Prefix: CMM **ID:** 0832

  User Response
  Replace the I/O module.

- **40040102 : I/O module [arg1] VPD is not valid.**

  The vital product data (VPD) of the specified I/O module is not valid. VPD includes information such as the serial number and part number to uniquely identify the I/O module.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  I/O Modules (Warning)

  SNMP Trap ID
  mmTrapION

  CIM Information
  Prefix: CMM **ID:** 0832

  User Response
  Replace the I/O module.

- **40040103 : I/O module [arg1] VPD is not valid.**

  The vital product data (VPD) of the specified I/O module is not valid. VPD includes information such as the serial number and part number to uniquely identify the I/O module.

  Severity
  Warning

  Serviceable
  Yes

Automatically notify support
Yes

Alert Category
I/O Modules (Warning)

SNMP Trap ID
mmTrapION

CIM Information
Prefix: CMM **ID:** 0832

User Response
Replace the I/O module.

- **40040104 : I/O module [arg1] VPD is not valid.**

  The vital product data (VPD) of the specified I/O module is not valid. VPD includes information such as the serial number and part number to uniquely identify the I/O module.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  I/O Modules (Warning)

  SNMP Trap ID
  mmTrapION

  CIM Information
  Prefix: CMM **ID:** 0832

  User Response
  Replace the I/O module.

- **40040201 : Chassis Management Module [arg1] VPD is not valid.**

  The vital product data (VPD) of the specified Chassis Management Module (CMM) is not valid. VPD includes information such as the serial number and part number to uniquely identify the CMM.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0833

  User Response
  Replace the Chassis Management Module.

- **40040202 : Chassis Management Module [arg1] VPD is not valid.**

  The vital product data (VPD) of the specified Chassis Management Module (CMM) is not valid. VPD includes information such as the serial number and part number to uniquely identify the CMM.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0833

  User Response
  Replace the Chassis Management Module.
- **40040401 : Chassis Management Module [arg1] VPD is not available.**

  The vital product data (VPD) of the specified Chassis Management Module (CMM) is not available. VPD includes information such as the serial number and part number to uniquely identify the CMM.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0834

  User Response
  Replace the Chassis Management Module.
- **40040402 : Chassis Management Module [arg1] VPD is not available.**

  The vital product data (VPD) of the specified Chassis Management Module (CMM) is not available. VPD includes information such as the serial number and part number to uniquely identify the CMM.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0834

User Response
Replace the Chassis Management Module.

- **40040501 : Chassis Management Module [arg1] is not compatible. Redundant capability is turned off.**

  Standby Chassis Management Module is not compliant with the specifications of the Flex System. Redundant capability is turned off.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0853

  User Response
  Replace the Chassis Management Module.

- **40040502 : Chassis Management Module [arg1] is not compatible. Redundant capability is turned off.**

  Standby Chassis Management Module is not compliant with the specifications of the Flex System. Redundant capability is turned off.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0853

  User Response
  Replace the Chassis Management Module.

- **40050000 : Hot air exiting from the rear of the chassis is recirculated in the inlet air at the front of the chassis. High Temperature: [arg1], Low Temperature: [arg2].**

  The front of this chassis has multiple node and chassis ambient air temperature sensors. If the inlet air temperature range across all these sensors becomes greater than the preset acceptable limit then this warning is triggered. This large inlet air temperature range indicates that some components will become warmer which in turn will request for more cooling, consuming more fan power than necessary.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0862

  User Response
  - First check to ensure the rack's sill-plate/rack-skirt/tilt-plate/baffle is installed at the front edge of the rack bottom. Common causes for this event are due to either cold or hot air escaping from under the rack and reaching the bottom-most ambient temperature sensors. If it is cold air that is the root cause, see last item.
  - To pinpoint the area that is creating this large ambient air temperature range, access the CMM's web browser to view and record each node and chassis ambient temperature readings. Note the physical locations of both the hottest and coldest ambient temperature readings. These are the two areas that need to be more closely studied.Look for any openings that permit rack's hot exhaust air to recirculate to the rack front. This can range from possible cable raceway caps being removed to missing filler/blank panels between servers and switches. In some cases, it was observed that the current rack was properly sealed but the adjacent rack had openings allowing hot air from the exhaust aisle to recirculate to rack front.
  - Once the opening has been pinpointed, plug it to verify the event recovers by observing system health and the CMM event log. If the rack configuration or datacenter layout does not permit the hot air from recirculating, then disable this event for the short term until a long term fix is implemented. To disable this hot air recirculating event, select the "Chassis management" in the CMM's web browser. Select "Chassis" then choose the "Temperature" tab followed by selecting the "Hot Air Recirculation" tab. Un-check the box and click "apply."
  - Regarding the cold air escaping from under the rack situation, this condition will not drive fans to higher speeds. Instead this condition reflects less than ideal sealing from the raised floor and rack cabling. Its recommended that the sealing is improved. However, if this is not realistic, one can revert to simply turning off the hot air recirculation detection event as described above on the bottom-most chassis in the rack to prevent this event. However, its still recommended to leave the hot air recirculation detection event enabled on the chassis above the bottom chassis to monitor for other possible hot air recirculating causes.
- **40050001 : Chassis Management Module [arg1] is not correctly connected to the chassis.**

  The Chassis Management Module (CMM) is not correctly installed in the chassis, or there is a problem with a connector.

  Severity
  Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0197

User Response
Complete the following steps until the problem is solved:

1. Make sure that the CMM is fully seated in the chassis.
2. Remove the CMM from the chassis and check for bent pins on the connectors. If there are bent pins, submit a service request, and do not reinstall the CMM in any CMM bay in the chassis.
3. Submit a service request.

- **40050002 : Chassis Management Module [arg1] is not correctly connected to the chassis.**

The Chassis Management Module (CMM) is not correctly installed in the chassis, or there is a problem with a connector.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0197

User Response
Complete the following steps until the problem is solved:

1. Make sure that the CMM is fully seated in the chassis.
2. Remove the CMM from the chassis and check for bent pins on the connectors. If there are bent pins, submit a service request, and do not reinstall the CMM in any CMM bay in the chassis.
3. Submit a service request.

- **40050003 : Hot air recirculation detection was enabled by user ID [arg1] from [arg2] at IP address [arg3].**

The specified user has enabled hot air recirculation detection.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0901

User Response
Information only; no action is required.

- **40050004 : The temperature threshold for hot air recirculation detection has been changed to [arg1] by [arg2] from [arg3] ([arg4]).**

  The specified user has changed the temperature delta threshold used to determine if hot air recirculation has occurred.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0681

  User Response
  Information only; no action is required.

- **40050005 : Hot air recirculation detection was disabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has disable hot air recirculation detection.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0902

  User Response

Information only; no action is required.

- **40050081 : Chassis power limit policy has been [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the chassis power limit policy.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0621

  User Response
  Information only; no action is required.

- **400F0001 : Node [arg1] device [arg2][[arg3]] VPD was changed.**

  The vital product data in the node has been changed.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0748

  User Response
  Information only; no action is required.

- **400F0002 : Node [arg1] device [arg2][[arg3]] VPD was changed.**

  The vital product data in the node has been changed.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category

Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0748

User Response
Information only; no action is required.

- **400F0003 : Node [arg1] device [arg2][[arg3]] VPD was changed.**

The vital product data in the node has been changed.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0748

User Response
Information only; no action is required.

- **400F0004 : Node [arg1] device [arg2][[arg3]] VPD was changed.**

The vital product data in the node has been changed.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0748

User Response
Information only; no action is required.

- **400F0005 : Node [arg1] device [arg2][[arg3]] VPD was changed.**

The vital product data in the node has been changed.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0748

User Response
Information only; no action is required.

- **400F0006 : Node [arg1] device [arg2][[arg3]] VPD was changed.**

The vital product data in the node has been changed.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0748

User Response
Information only; no action is required.

- **400F0007 : Node [arg1] device [arg2][[arg3]] VPD was changed.**

The vital product data in the node has been changed.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0748

User Response

Information only; no action is required.

- **400F0008 : Node [arg1] device [arg2][[arg3]] VPD was changed.**

  The vital product data in the node has been changed.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0748

  User Response
  Information only; no action is required.

- **400F0009 : Node [arg1] device [arg2][[arg3]] VPD was changed.**

  The vital product data in the node has been changed.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0748

  User Response
  Information only; no action is required.

- **400F000A : Node [arg1] device [arg2][[arg3]] VPD was changed.**

  The vital product data in the node has been changed.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0748

User Response
Information only; no action is required.

- **400F000B : Node [arg1] device [arg2][[arg3]] VPD was changed.**

  The vital product data in the node has been changed.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0748

  User Response
  Information only; no action is required.
- **400F000C : Node [arg1] device [arg2][[arg3]] VPD was changed.**

  The vital product data in the node has been changed.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0748

  User Response
  Information only; no action is required.
- **400F000D : Node [arg1] device [arg2][[arg3]] VPD was changed.**

  The vital product data in the node has been changed.

  Severity
  Informational

  Serviceable

No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0748

User Response
Information only; no action is required.

- **400F000E : Node [arg1] device [arg2][[arg3]] VPD was changed.**

  The vital product data in the node has been changed.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0748

  User Response
  Information only; no action is required.

- **40110001 : CMM IPv6 configuration changed, [arg1] IP address [arg2].**

  An IPv6 address has been added to or removed from the list of addresses that the Chassis Management Module can respond to. The address can be static, autoconfig, or DHCP. A separate event is provided when an IP address has been added via DHCPv6.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Network change (Informational)

  SNMP Trap ID
  mmTrapNwChangeS

  CIM Information
  Prefix: CMM **ID:** 0192

User Response
Information only; no action is required.

- **40110002 : IPv6 static configuration for [arg1] CMM has been set: IP=[arg2], prefix=[arg3], gateway=[arg4].**

  The specified IPv6 static configuration of the Chassis Management Module external network interface has been applied.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Network change (Informational)

  SNMP Trap ID
  mmTrapNwChangeS

  CIM Information
  Prefix: CMM **ID:** 0570

  User Response
  Information only; no action is required.

- **40110004 : Floating IPv6 configuration for [arg1] CMM has been set: IP=[arg2], prefix=[arg3], gateway=[arg4].**

  The specified floating IPv6 configuration of the Chassis Management Module external network interface has been applied.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Network change (Informational)

  SNMP Trap ID
  mmTrapNwChangeS

  CIM Information
  Prefix: CMM **ID:** 0642

  User Response
  Information only; no action is required.

- **40110005 : CMM floating IPv6 configuration [arg1] to IP address [arg2].**

  The floating IPv6 address has been added to or removed from the list of addresses that the Chassis Management Module can respond to.

  Severity
  Informational

  Serviceable

No

Automatically notify support
No

Alert Category
Network change (Informational)

SNMP Trap ID
mmTrapNwChangeS

CIM Information
Prefix: CMM **ID:** 0199

User Response
Information only; no action is required.

- **40217006 : Logical uplink failover IPv4 address setting has been changed by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has changed the "Failover IPv4 address for logical link loss" setting.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0535

  User Response
  Information only; no action is required.

- **40217007 : Logical uplink failover IPv6 address setting for [arg1] CMM has been changed by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the "Failover IPv6 address for logical link loss" setting.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0575

User Response
Information only; no action is required.

- **40217008 : Logical uplink failover policy setting has been changed by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has changed the "Failover policy for logical link loss" setting.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0536

  User Response
  Information only; no action is required.

- **40217009 : Standby Chassis Management Module external network physical link broken.**

  The standby Chassis Management Module (CMM) physical link to the external network has been broken.

  Severity
  Warning

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0815

  User Response
  Complete the following steps until the problem is solved:

  1. Make sure that the Ethernet cable is connected (check the connections on both ends of the cable) and that the cable is intact.
  2. Make sure that the devices on both ends of the cable are powered on and functioning.

- **4021700A : Standby Chassis Management Module external network logical link broken.**

  The standby Chassis Management Module (CMM) logical link to the external network has been broken.

  Severity
  Warning

  Serviceable

Yes

Automatically notify support
No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0816

User Response
Make sure that the network is configured correctly and is functioning.

- **40324001 : IPv6 was enabled on I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has requested that IPv6 to be enabled for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0978

  User Response
  Information only; no action is required.

- **40324002 : IPv6 was enabled on I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has requested that IPv6 to be enabled for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0978

User Response
Information only; no action is required.

- **40324003 : IPv6 was enabled on I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has requested that IPv6 to be enabled for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0978

  User Response
  Information only; no action is required.

- **40324004 : IPv6 was enabled on I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has requested that IPv6 to be enabled for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0978

  User Response
  Information only; no action is required.

- **40324101 : IPv6 was disabled on I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has requested that IPv6 to be disabled for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0979

User Response
Information only; no action is required.

- **40324102 : IPv6 was disabled on I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has requested that IPv6 to be disabled for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0979

  User Response
  Information only; no action is required.

- **40324103 : IPv6 was disabled on I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has requested that IPv6 to be disabled for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0979

  User Response
  Information only; no action is required.

- **40324104 : IPv6 was disabled on I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has requested that IPv6 to be disabled for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0979

  User Response
  Information only; no action is required.
- **40324201 : IPv6 static configuration was enabled for I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has requested that IPv6 static configuration to be enabled for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0972

  User Response
  Information only; no action is required.
- **40324202 : IPv6 static configuration was enabled for I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has requested that IPv6 static configuration to be enabled for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0972

User Response
Information only; no action is required.

- **40324203 : IPv6 static configuration was enabled for I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has requested that IPv6 static configuration to be enabled for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0972

  User Response
  Information only; no action is required.

- **40324204 : IPv6 static configuration was enabled for I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has requested that IPv6 static configuration to be enabled for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0972

  User Response
  Information only; no action is required.

- **40324211 : IPv6 static configuration was disabled for I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

The specified user has requested that IPv6 static configuration to be disabled for the specified I/O module.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0973

User Response
Information only; no action is required.

- **40324212 : IPv6 static configuration was disabled for I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has requested that IPv6 static configuration to be disabled for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0973

  User Response
  Information only; no action is required.

- **40324213 : IPv6 static configuration was disabled for I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has requested that IPv6 static configuration to be disabled for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0973

User Response
Information only; no action is required.

- **40324214 : IPv6 static configuration was disabled for I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has requested that IPv6 static configuration to be disabled for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0973

  User Response
  Information only; no action is required.

- **40324301 : IPv6 DHCP configuration was enabled for I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has requested that IPv6 DHCP configuration to be enabled for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0974

  User Response
  Information only; no action is required.

- **40324302 : IPv6 DHCP configuration was enabled for I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has requested that IPv6 DHCP configuration to be enabled for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0974

  User Response
  Information only; no action is required.
- **40324303 : IPv6 DHCP configuration was enabled for I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has requested that IPv6 DHCP configuration to be enabled for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0974

  User Response
  Information only; no action is required.
- **40324304 : IPv6 DHCP configuration was enabled for I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has requested that IPv6 DHCP configuration to be enabled for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0974

User Response
Information only; no action is required.

- **40324311 : IPv6 DHCP configuration was disabled for I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has requested that IPv6 DHCP configuration to be disabled for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0975

  User Response
  Information only; no action is required.

- **40324312 : IPv6 DHCP configuration was disabled for I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has requested that IPv6 DHCP configuration to be disabled for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0975

User Response
Information only; no action is required.

- **40324313 : IPv6 DHCP configuration was disabled for I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has requested that IPv6 DHCP configuration to be disabled for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0975

  User Response
  Information only; no action is required.

- **40324314 : IPv6 DHCP configuration was disabled for I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has requested that IPv6 DHCP configuration to be disabled for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0975

  User Response
  Information only; no action is required.

- **40324401 : IPv6 stateless auto-configuration was enabled for I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has requested that IPv6 stateless automatic configuration to be enabled for the specified I/O module.

  Severity
  Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0976

User Response
Information only; no action is required.

- **40324402 : IPv6 stateless auto-configuration was enabled for I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has requested that IPv6 stateless automatic configuration to be enabled for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0976

  User Response
  Information only; no action is required.

- **40324403 : IPv6 stateless auto-configuration was enabled for I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has requested that IPv6 stateless automatic configuration to be enabled for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0976

User Response
Information only; no action is required.

- **40324404 : IPv6 stateless auto-configuration was enabled for I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has requested that IPv6 stateless automatic configuration to be enabled for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0976

  User Response
  Information only; no action is required.

- **40324411 : IPv6 stateless auto-configuration was disabled for I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has requested that IPv6 stateless automatic configuration to be disabled for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0977

  User Response
  Information only; no action is required.

- **40324412 : IPv6 stateless auto-configuration was disabled for I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has requested that IPv6 stateless automatic configuration to be disabled for the specified I/O module.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0977

User Response
Information only; no action is required.

- **40324413 : IPv6 stateless auto-configuration was disabled for I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has requested that IPv6 stateless automatic configuration to be disabled for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0977

  User Response
  Information only; no action is required.

- **40324414 : IPv6 stateless auto-configuration was disabled for I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has requested that IPv6 stateless automatic configuration to be disabled for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0977

User Response
Information only; no action is required.

- **40324501 : IPv6 static address was changed to [arg1] for I/O module [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IPv6 static address for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0183

  User Response
  Information only; no action is required.

- **40324502 : IPv6 static address was changed to [arg1] for I/O module [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IPv6 static address for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0183

  User Response
  Information only; no action is required.

- **40324503 : IPv6 static address was changed to [arg1] for I/O module [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IPv6 static address for the specified I/O module.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0183

User Response
Information only; no action is required.

- **40324504 : IPv6 static address was changed to [arg1] for I/O module [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IPv6 static address for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0183

  User Response
  Information only; no action is required.

- **40324601 : IPv6 gateway address was changed to [arg1] for I/O module [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IPv6 gateway address for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0184

User Response
Information only; no action is required.

- **40324602 : IPv6 gateway address was changed to [arg1] for I/O module [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IPv6 gateway address for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0184

  User Response
  Information only; no action is required.

- **40324603 : IPv6 gateway address was changed to [arg1] for I/O module [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IPv6 gateway address for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0184

  User Response
  Information only; no action is required.

- **40324604 : IPv6 gateway address was changed to [arg1] for I/O module [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IPv6 gateway address for the specified I/O module.

  Severity
  Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0184

User Response
Information only; no action is required.

- **40324701 : IPv6 prefix length was changed to [arg1] for I/O module [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IPv6 prefix length for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0185

  User Response
  Information only; no action is required.

- **40324702 : IPv6 prefix length was changed to [arg1] for I/O module [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IPv6 prefix length for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0185

User Response
Information only; no action is required.

- **40324703 : IPv6 prefix length was changed to [arg1] for I/O module [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IPv6 prefix length for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0185

  User Response
  Information only; no action is required.

- **40324704 : IPv6 prefix length was changed to [arg1] for I/O module [arg2] by user ID [arg3] from [arg4] at IP address [arg5].**

  The specified user has changed the IPv6 prefix length for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0185

  User Response
  Information only; no action is required.

- **40324801 : Configuration request succeeded for I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has successfully changed the configuration for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0186

User Response
Information only; no action is required.

- **40324802 : Configuration request succeeded for I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has successfully changed the configuration for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0186

  User Response
  Information only; no action is required.

- **40324803 : Configuration request succeeded for I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has successfully changed the configuration for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0186

  User Response
  Information only; no action is required.

- **40324804 : Configuration request succeeded for I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has successfully changed the configuration for the specified I/O module.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0186

  User Response
  Information only; no action is required.
- **40324901 : Configuration request failed for I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user was not able to change the IPv6 configuration for the specified I/O module.

  Severity
  Informational

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0187

  User Response
  Complete the following steps until the problem is solved:

  1. Try the configuration change again.
  2. Make sure that the I/O module is capable of IPv6 configuration. See the I/O-module documentation.
  3. Use the I/O-module external interfaces to change the address.
- **40324902 : Configuration request failed for I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user was not able to change the IPv6 configuration for the specified I/O module.

  Severity
  Informational

Serviceable
Yes

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0187

User Response
Complete the following steps until the problem is solved:

1. Try the configuration change again.
2. Make sure that the I/O module is capable of IPv6 configuration. See the I/O-module documentation.
3. Use the I/O-module external interfaces to change the address.

- **40324903 : Configuration request failed for I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user was not able to change the IPv6 configuration for the specified I/O module.

  Severity
  Informational

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0187

  User Response
  Complete the following steps until the problem is solved:

  1. Try the configuration change again.
  2. Make sure that the I/O module is capable of IPv6 configuration. See the I/O-module documentation.
  3. Use the I/O-module external interfaces to change the address.

- **40324904 : Configuration request failed for I/O module [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user was not able to change the IPv6 configuration for the specified I/O module.

  Severity
  Informational

  Serviceable
  Yes

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0187

User Response
Complete the following steps until the problem is solved:

1. Try the configuration change again.
2. Make sure that the I/O module is capable of IPv6 configuration. See the I/O-module documentation.
3. Use the I/O-module external interfaces to change the address.

- **40324A01 : DHCP configuration timeout for I/O module [arg1].**

The specified I/O-module DHCP configuration has timed out. See the I/O-module documentation.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0188

User Response
Information only; no action is required.

- **40324A02 : DHCP configuration timeout for I/O module [arg1].**

The specified I/O-module DHCP configuration has timed out. See the I/O-module documentation.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information

Prefix: CMM **ID:** 0188

User Response
Information only; no action is required.

- **40324A03 : DHCP configuration timeout for I/O module [arg1].**

  The specified I/O-module DHCP configuration has timed out. See the I/O-module documentation.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0188

  User Response
  Information only; no action is required.

- **40324A04 : DHCP configuration timeout for I/O module [arg1].**

  The specified I/O-module DHCP configuration has timed out. See the I/O-module documentation.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0188

  User Response
  Information only; no action is required.

- **40524901 : I/O module [arg1] POST retry.**

  The Chassis Management Module performs POST retry to the specified I/O module because POST timeout.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support

No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0246

User Response
Information only; no action is required. If this condition persists, check for other applicable messages or a successful I/O module POST code in the CMM or Flex System Manager event log.

- **40524902 : I/O module [arg1] POST retry.**

The Chassis Management Module performs POST retry to the specified I/O module because POST timeout.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0246

User Response
Information only; no action is required. If this condition persists, check for other applicable messages or a successful I/O module POST code in the CMM or Flex System Manager event log.

- **40524903 : I/O module [arg1] POST retry.**

The Chassis Management Module performs POST retry to the specified I/O module because POST timeout.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
I/O Modules (Informational)

SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM **ID:** 0246

User Response

Information only; no action is required. If this condition persists, check for other applicable messages or a successful I/O module POST code in the CMM or Flex System Manager event log.

- **40524904 : I/O module [arg1] POST retry.**

  The Chassis Management Module performs POST retry to the specified I/O module because POST timeout.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  I/O Modules (Informational)

  SNMP Trap ID
  mmTrapIOS

  CIM Information
  Prefix: CMM **ID:** 0246

  User Response
  Information only; no action is required. If this condition persists, check for other applicable messages or a successful I/O module POST code in the CMM or Flex System Manager event log.

- **40625001 : Node [arg1] system-management processor failed initialization to allow monitoring.**

  The system-management processor of the specified node did not provide adequate information during the initialization sequence. The node will not be monitored.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Critical)

  SNMP Trap ID
  mmTrapBladeC

  CIM Information
  Prefix: CMM **ID:** 0718

  User Response
  Complete the following steps until the problem is solved:

  1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
  2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
  3. Perform a hard restart of the node system-management processor.

4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **40625002 : Node [arg1] system-management processor failed initialization to allow monitoring.**

  The system-management processor of the specified node did not provide adequate information during the initialization sequence. The node will not be monitored.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Critical)

  SNMP Trap ID
  mmTrapBladeC

  CIM Information
  Prefix: CMM **ID:** 0718

  User Response
  Complete the following steps until the problem is solved:

  1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
  2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
  3. Perform a hard restart of the node system-management processor.
  4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **40625003 : Node [arg1] system-management processor failed initialization to allow monitoring.**

  The system-management processor of the specified node did not provide adequate information during the initialization sequence. The node will not be monitored.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Critical)

  SNMP Trap ID
  mmTrapBladeC

  CIM Information
  Prefix: CMM **ID:** 0718

User Response

Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.
4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **40625004 : Node [arg1] system-management processor failed initialization to allow monitoring.**

The system-management processor of the specified node did not provide adequate information during the initialization sequence. The node will not be monitored.

Severity

Error

Serviceable

Yes

Automatically notify support

No

Alert Category

Nodes (Critical)

SNMP Trap ID

mmTrapBladeC

CIM Information

Prefix: CMM **ID:** 0718

User Response

Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.
4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **40625005 : Node [arg1] system-management processor failed initialization to allow monitoring.**

The system-management processor of the specified node did not provide adequate information during the initialization sequence. The node will not be monitored.

Severity

Error

Serviceable

Yes

Automatically notify support
No

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0718

User Response
Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.
4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **40625006 : Node [arg1] system-management processor failed initialization to allow monitoring.**

The system-management processor of the specified node did not provide adequate information during the initialization sequence. The node will not be monitored.

Severity
Error

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0718

User Response
Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.

4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **40625007 : Node [arg1] system-management processor failed initialization to allow monitoring.**

  The system-management processor of the specified node did not provide adequate information during the initialization sequence. The node will not be monitored.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Critical)

  SNMP Trap ID
  mmTrapBladeC

  CIM Information
  Prefix: CMM **ID:** 0718

  User Response
  Complete the following steps until the problem is solved:

  1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
  2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
  3. Perform a hard restart of the node system-management processor.
  4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **40625008 : Node [arg1] system-management processor failed initialization to allow monitoring.**

  The system-management processor of the specified node did not provide adequate information during the initialization sequence. The node will not be monitored.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Critical)

  SNMP Trap ID
  mmTrapBladeC

  CIM Information
  Prefix: CMM **ID:** 0718

User Response

Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.
4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **40625009 : Node [arg1] system-management processor failed initialization to allow monitoring.**

The system-management processor of the specified node did not provide adequate information during the initialization sequence. The node will not be monitored.

Severity

Error

Serviceable

Yes

Automatically notify support

No

Alert Category

Nodes (Critical)

SNMP Trap ID

mmTrapBladeC

CIM Information

Prefix: CMM **ID:** 0718

User Response

Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.
4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **4062500A : Node [arg1] system-management processor failed initialization to allow monitoring.**

The system-management processor of the specified node did not provide adequate information during the initialization sequence. The node will not be monitored.

Severity

Error

Serviceable

Yes

Automatically notify support
No

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0718

User Response
Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.
4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **4062500B : Node [arg1] system-management processor failed initialization to allow monitoring.**

The system-management processor of the specified node did not provide adequate information during the initialization sequence. The node will not be monitored.

Severity
Error

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0718

User Response
Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.

4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **4062500C : Node [arg1] system-management processor failed initialization to allow monitoring.**

  The system-management processor of the specified node did not provide adequate information during the initialization sequence. The node will not be monitored.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Critical)

  SNMP Trap ID
  mmTrapBladeC

  CIM Information
  Prefix: CMM **ID:** 0718

  User Response
  Complete the following steps until the problem is solved:

  1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
  2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
  3. Perform a hard restart of the node system-management processor.
  4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **4062500D : Node [arg1] system-management processor failed initialization to allow monitoring.**

  The system-management processor of the specified node did not provide adequate information during the initialization sequence. The node will not be monitored.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Nodes (Critical)

  SNMP Trap ID
  mmTrapBladeC

  CIM Information
  Prefix: CMM **ID:** 0718

User Response

Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.
4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **4062500E : Node [arg1] system-management processor failed initialization to allow monitoring.**

The system-management processor of the specified node did not provide adequate information during the initialization sequence. The node will not be monitored.

Severity

Error

Serviceable

Yes

Automatically notify support

No

Alert Category

Nodes (Critical)

SNMP Trap ID

mmTrapBladeC

CIM Information

Prefix: CMM **ID:** 0718

User Response

Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.
4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **4300010E : Complex Descriptor obtained from [arg1] is corrupted. No impact unless all nodes of complex have same error.**

The compute node provided a complex descriptor that is not valid. This will not be an impact unless all compute nodes of the same complex also have this error. If any node does provide a good complex descriptor, that will sufficient for the management module support of partition data.

Severity

Informational

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM **ID:** 0694

User Response
Perform these steps if all the nodes of a complex have this error:

1. Reset the node system management processor on all compute nodes in the scalable node complex. You can reset the service processor through the chassis management module Web interface from the Node Power/Restart page.
2. Disconnect the SMP connector and reseat the scalable nodes of the complex.
3. Update the firmware for the service processor on the specified compute node server. You can find the appropriate firmware on the Flex software and device drivers Web page.

- **48008401 : Power allocated is higher than the power capacity in power domain [arg1].**

The power that has been allocated to the components in the chassis exceeds the available power capacity of the chassis.

Severity
Warning

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0195

User Response
Information only; no action is required.

- **4800A400 : Node power policy on chassis restart changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

The specified user has changed the power policy for nodes in the chassis. The new policy will take effect when the Chassis Management Module is restarted.

Severity
Informational

Serviceable
No

Automatically notify support

No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0282

User Response
Information only; no action is required.

- **4800A401 : Node power restoration delay on chassis restart changed to [arg1] by user ID [arg2] from [arg3] at IP address [arg4].**

  The specified user has changed the power restoration delay for nodes in the chassis. The new setting will take effect when the chassis is power cycled.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0266

  User Response
  Information only; no action is required.

- **50020000 : Not reading device on system management (I2C) bus [arg1]. Chassis Management Module in the chassis [arg2] communication is offline.**

  The Chassis Management Module is not able to communicate with any device.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0124

  User Response
  Replace the Chassis Management Module.

- **50020101 : Not reading device on system management (I2C) bus [arg1]. The rear LED card in the chassis [arg2] communication is offline.**

  The Chassis Management Module (CMM) is not able to communicate with the rear LED card.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0125

  User Response
  If the chassis has one CMM, replace the CMM. If the problem remains, replace the rear LED card. As a potential temporary workaround, try to move the CMM to the other CMM bay. If the chassis has two CMMs, replace the rear LED card.
- **50020102 : Not reading device on system management (I2C) bus [arg1]. The rear LED card in the chassis [arg2] communication is offline.**

  The Chassis Management Module (CMM) is not able to communicate with the rear LED card.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0125

  User Response
  If the chassis has one CMM, replace the CMM. If the problem remains, replace the rear LED card. As a potential temporary workaround, try to move the CMM to the other CMM bay. If the chassis has two CMMs, replace the rear LED card.
- **50020201 : Not reading device on system management (I2C) bus [arg1]. Fan logic module [arg2] communication is offline.**

  The Chassis Management Module is not able to communicate with the fan logic module.

  Severity
  Error

  Serviceable

Yes

Automatically notify support
Yes

Alert Category
Chassis/System Management (Critical)

SNMP Trap ID
mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0126

User Response
Replace the fan logic module. If the problem remains, replace the CMM.

- **50020202 : Not reading device on system management (I2C) bus [arg1]. Fan logic module [arg2] communication is offline.**

  The Chassis Management Module is not able to communicate with the fan logic module.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0126

  User Response
  Replace the fan logic module. If the problem remains, replace the CMM.

- **50020281 : Not reading device on system management (I2C) bus [arg1]. Fan logic module [arg2] VPD communication is offline.**

  The Chassis Management Module is not able to read the vital product data (VPD) on the fan logic module.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0127

User Response
Replace the fan logic module.

- **50020282 : Not reading device on system management (I2C) bus [arg1]. Fan logic module [arg2] VPD communication is offline.**

  The Chassis Management Module is not able to read the vital product data (VPD) on the fan logic module.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0127

  User Response
  Replace the fan logic module.

- **50020301 : Not reading device on system management (I2C) bus [arg1]. I/O module [arg2] communication is offline.**

  The Chassis Management Module is not able to communicate with the I/O module on the I2C bus.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0128

  User Response
  Perform a service-level reset of the I/O module. If the problem remains, replace the I/O module.

- **50020302 : Not reading device on system management (I2C) bus [arg1]. I/O module [arg2] communication is offline.**

  The Chassis Management Module is not able to communicate with the I/O module on the I2C bus.

  Severity
  Error

  Serviceable
  Yes

Automatically notify support
Yes

Alert Category
Chassis/System Management (Critical)

SNMP Trap ID
mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0128

User Response
Perform a service-level reset of the I/O module. If the problem remains, replace the I/O module.

- **50020303 : Not reading device on system management (I2C) bus [arg1]. I/O module [arg2] communication is offline.**

  The Chassis Management Module is not able to communicate with the I/O module on the I2C bus.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0128

  User Response
  Perform a service-level reset of the I/O module. If the problem remains, replace the I/O module.

- **50020304 : Not reading device on system management (I2C) bus [arg1]. I/O module [arg2] communication is offline.**

  The Chassis Management Module is not able to communicate with the I/O module on the I2C bus.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0128

  User Response
  Perform a service-level reset of the I/O module. If the problem remains, replace the I/O module.

- **50020401 : Not reading device on system management (I2C) bus [arg1]. Fan module [arg2] communication is offline.**

  The Chassis Management Module (CMM) is not able to communicate with the specified fan module. If there is an error in a fan logic module, the CMM cannot monitor the associated fan modules or detect their presence, and the fan modules on that side of the chassis will speed up. Solve fan logic module issues before you address fan-module issues.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0129

  User Response
  Replace the fan module.
- **50020402 : Not reading device on system management (I2C) bus [arg1]. Fan module [arg2] communication is offline.**

  The Chassis Management Module (CMM) is not able to communicate with the specified fan module. If there is an error in a fan logic module, the CMM cannot monitor the associated fan modules or detect their presence, and the fan modules on that side of the chassis will speed up. Solve fan logic module issues before you address fan-module issues.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0129

  User Response
  Replace the fan module.
- **50020403 : Not reading device on system management (I2C) bus [arg1]. Fan module [arg2] communication is offline.**

  The Chassis Management Module (CMM) is not able to communicate with the specified fan module. If there is an error in a fan logic module, the CMM cannot monitor the associated fan modules or detect their

presence, and the fan modules on that side of the chassis will speed up. Solve fan logic module issues before you address fan-module issues.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Chassis/System Management (Critical)

SNMP Trap ID
mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0129

User Response
Replace the fan module.

- **50020404 : Not reading device on system management (I2C) bus [arg1]. Fan module [arg2] communication is offline.**

  The Chassis Management Module (CMM) is not able to communicate with the specified fan module. If there is an error in a fan logic module, the CMM cannot monitor the associated fan modules or detect their presence, and the fan modules on that side of the chassis will speed up. Solve fan logic module issues before you address fan-module issues.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0129

  User Response
  Replace the fan module.

- **50020405 : Not reading device on system management (I2C) bus [arg1]. Fan module [arg2] communication is offline.**

  The Chassis Management Module (CMM) is not able to communicate with the specified fan module. If there is an error in a fan logic module, the CMM cannot monitor the associated fan modules or detect their presence, and the fan modules on that side of the chassis will speed up. Solve fan logic module issues before you address fan-module issues.

  Severity
  Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Chassis/System Management (Critical)

SNMP Trap ID
mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0129

User Response
Replace the fan module.

- **50020406 : Not reading device on system management (I2C) bus [arg1]. Fan module [arg2] communication is offline.**

  The Chassis Management Module (CMM) is not able to communicate with the specified fan module. If there is an error in a fan logic module, the CMM cannot monitor the associated fan modules or detect their presence, and the fan modules on that side of the chassis will speed up. Solve fan logic module issues before you address fan-module issues.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0129

  User Response
  Replace the fan module.

- **50020407 : Not reading device on system management (I2C) bus [arg1]. Fan module [arg2] communication is offline.**

  The Chassis Management Module (CMM) is not able to communicate with the specified fan module. If there is an error in a fan logic module, the CMM cannot monitor the associated fan modules or detect their presence, and the fan modules on that side of the chassis will speed up. Solve fan logic module issues before you address fan-module issues.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category

Chassis/System Management (Critical)

SNMP Trap ID
mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0129

User Response
Replace the fan module.

- **50020408 : Not reading device on system management (I2C) bus [arg1]. Fan module [arg2] communication is offline.**

  The Chassis Management Module (CMM) is not able to communicate with the specified fan module. If there is an error in a fan logic module, the CMM cannot monitor the associated fan modules or detect their presence, and the fan modules on that side of the chassis will speed up. Solve fan logic module issues before you address fan-module issues.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0129

  User Response
  Replace the fan module.

- **50020409 : Not reading device on system management (I2C) bus [arg1]. Fan module [arg2] communication is offline.**

  The Chassis Management Module (CMM) is not able to communicate with the specified fan module. If there is an error in a fan logic module, the CMM cannot monitor the associated fan modules or detect their presence, and the fan modules on that side of the chassis will speed up. Solve fan logic module issues before you address fan-module issues.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0129

User Response
Replace the fan module.

- **5002040A : Not reading device on system management (I2C) bus [arg1]. Fan module [arg2] communication is offline.**

  The Chassis Management Module (CMM) is not able to communicate with the specified fan module. If there is an error in a fan logic module, the CMM cannot monitor the associated fan modules or detect their presence, and the fan modules on that side of the chassis will speed up. Solve fan logic module issues before you address fan-module issues.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0129

  User Response
  Replace the fan module.

- **50020501 : Not reading device on system management (I2C) bus [arg1]. Power supply [arg2] communication is offline.**

  The Chassis Management Module (CMM) is not able to communicate with the power supply.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0130

  User Response
  If multiple power supplies are offline, replace the CMM. Otherwise, replace the power supply.

- **50020502 : Not reading device on system management (I2C) bus [arg1]. Power supply [arg2] communication is offline.**

  The Chassis Management Module (CMM) is not able to communicate with the power supply.

  Severity
  Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Chassis/System Management (Critical)

SNMP Trap ID
mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0130

User Response
If multiple power supplies are offline, replace the CMM. Otherwise, replace the power supply.

- **50020503 : Not reading device on system management (I2C) bus [arg1]. Power supply [arg2] communication is offline.**

The Chassis Management Module (CMM) is not able to communicate with the power supply.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Chassis/System Management (Critical)

SNMP Trap ID
mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0130

User Response
If multiple power supplies are offline, replace the CMM. Otherwise, replace the power supply.

- **50020504 : Not reading device on system management (I2C) bus [arg1]. Power supply [arg2] communication is offline.**

The Chassis Management Module (CMM) is not able to communicate with the power supply.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Chassis/System Management (Critical)

SNMP Trap ID
mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0130

User Response
If multiple power supplies are offline, replace the CMM. Otherwise, replace the power supply.

- **50020505 : Not reading device on system management (I2C) bus [arg1]. Power supply [arg2] communication is offline.**

  The Chassis Management Module (CMM) is not able to communicate with the power supply.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0130

  User Response
  If multiple power supplies are offline, replace the CMM. Otherwise, replace the power supply.

- **50020506 : Not reading device on system management (I2C) bus [arg1]. Power supply [arg2] communication is offline.**

  The Chassis Management Module (CMM) is not able to communicate with the power supply.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0130

  User Response
  If multiple power supplies are offline, replace the CMM. Otherwise, replace the power supply.

- **50020601 : Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.**

  The specified node is not able to communicate with the Chassis Management Module (CMM) on the I2C bus.

  Severity
  Error

  Serviceable
  Yes

Automatically notify support
Yes

Alert Category
Chassis/System Management (Critical)

SNMP Trap ID
mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0131

User Response
Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.
4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **50020602 : Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.**

The specified node is not able to communicate with the Chassis Management Module (CMM) on the I2C bus.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Chassis/System Management (Critical)

SNMP Trap ID
mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0131

User Response
Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.

4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **50020603 : Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.**

  The specified node is not able to communicate with the Chassis Management Module (CMM) on the I2C bus.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0131

  User Response
  Complete the following steps until the problem is solved:

  1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
  2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
  3. Perform a hard restart of the node system-management processor.
  4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **50020604 : Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.**

  The specified node is not able to communicate with the Chassis Management Module (CMM) on the I2C bus.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0131

User Response
Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.
4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **50020605 : Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.**

The specified node is not able to communicate with the Chassis Management Module (CMM) on the I2C bus.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Chassis/System Management (Critical)

SNMP Trap ID
mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0131

User Response
Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.
4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **50020606 : Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.**

The specified node is not able to communicate with the Chassis Management Module (CMM) on the I2C bus.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Chassis/System Management (Critical)

SNMP Trap ID
mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0131

User Response
Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.
4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **50020607 : Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.**

The specified node is not able to communicate with the Chassis Management Module (CMM) on the I2C bus.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Chassis/System Management (Critical)

SNMP Trap ID
mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0131

User Response
Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.

2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.
4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **50020608 : Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.**

  The specified node is not able to communicate with the Chassis Management Module (CMM) on the I2C bus.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0131

  User Response
  Complete the following steps until the problem is solved:

  1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
  2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
  3. Perform a hard restart of the node system-management processor.
  4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **50020609 : Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.**

  The specified node is not able to communicate with the Chassis Management Module (CMM) on the I2C bus.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

Alert Category
Chassis/System Management (Critical)

SNMP Trap ID
mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0131

User Response
Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.
4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **5002060A : Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.**

The specified node is not able to communicate with the Chassis Management Module (CMM) on the I2C bus.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Chassis/System Management (Critical)

SNMP Trap ID
mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0131

User Response
Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.
4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **5002060B : Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.**

  The specified node is not able to communicate with the Chassis Management Module (CMM) on the I2C bus.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0131

  User Response
  Complete the following steps until the problem is solved:

  1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
  2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
  3. Perform a hard restart of the node system-management processor.
  4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.
- **5002060C : Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.**

  The specified node is not able to communicate with the Chassis Management Module (CMM) on the I2C bus.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0131

User Response

Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.
4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **5002060D : Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.**

  The specified node is not able to communicate with the Chassis Management Module (CMM) on the I2C bus.

  Severity

  Error

  Serviceable

  Yes

  Automatically notify support

  Yes

  Alert Category

  Chassis/System Management (Critical)

  SNMP Trap ID

  mmTrapChassisC

  CIM Information

  Prefix: CMM **ID:** 0131

  User Response

  Complete the following steps until the problem is solved:

  1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
  2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
  3. Perform a hard restart of the node system-management processor.
  4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **5002060E : Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.**

  The specified node is not able to communicate with the Chassis Management Module (CMM) on the I2C bus.

  Severity

  Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Chassis/System Management (Critical)

SNMP Trap ID
mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0131

User Response
Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.
4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **50020701 : Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.**

The specified node is not able to communicate with the Chassis Management Module (CMM) on the I2C bus.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Chassis/System Management (Critical)

SNMP Trap ID
mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0131

User Response
Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.

3. Perform a hard restart of the node system-management processor.
4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **50020702 : Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.**

  The specified node is not able to communicate with the Chassis Management Module (CMM) on the I2C bus.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0131

  User Response
  Complete the following steps until the problem is solved:

  1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
  2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
  3. Perform a hard restart of the node system-management processor.
  4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **50020703 : Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.**

  The specified node is not able to communicate with the Chassis Management Module (CMM) on the I2C bus.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID

mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0131

User Response
Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.
4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **50020704 : Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.**

The specified node is not able to communicate with the Chassis Management Module (CMM) on the I2C bus.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Chassis/System Management (Critical)

SNMP Trap ID
mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0131

User Response
Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.
4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **50020705 : Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.**

The specified node is not able to communicate with the Chassis Management Module (CMM) on the I2C bus.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Chassis/System Management (Critical)

SNMP Trap ID
mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0131

User Response
Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.
4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **50020706 : Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.**

The specified node is not able to communicate with the Chassis Management Module (CMM) on the I2C bus.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Chassis/System Management (Critical)

SNMP Trap ID
mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0131

User Response
Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.
4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **50020707 : Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.**

  The specified node is not able to communicate with the Chassis Management Module (CMM) on the I2C bus.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0131

  User Response
  Complete the following steps until the problem is solved:

  1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
  2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
  3. Perform a hard restart of the node system-management processor.
  4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **50020708 : Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.**

  The specified node is not able to communicate with the Chassis Management Module (CMM) on the I2C bus.

  Severity
  Error

  Serviceable
  Yes

Automatically notify support
Yes

Alert Category
Chassis/System Management (Critical)

SNMP Trap ID
mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0131

User Response
Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.
4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **50020709 : Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.**

The specified node is not able to communicate with the Chassis Management Module (CMM) on the I2C bus.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Chassis/System Management (Critical)

SNMP Trap ID
mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0131

User Response
Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.

4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **5002070A : Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.**

  The specified node is not able to communicate with the Chassis Management Module (CMM) on the I2C bus.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

  CIM Information
  Prefix: CMM **ID:** 0131

  User Response
  Complete the following steps until the problem is solved:

  1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
  2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
  3. Perform a hard restart of the node system-management processor.
  4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **5002070B : Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.**

  The specified node is not able to communicate with the Chassis Management Module (CMM) on the I2C bus.

  Severity
  Error

  Serviceable
  Yes

  Automatically notify support
  Yes

  Alert Category
  Chassis/System Management (Critical)

  SNMP Trap ID
  mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0131

User Response
Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.
4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **5002070C : Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.**

The specified node is not able to communicate with the Chassis Management Module (CMM) on the I2C bus.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Chassis/System Management (Critical)

SNMP Trap ID
mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0131

User Response
Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.
4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **5002070D : Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.**

The specified node is not able to communicate with the Chassis Management Module (CMM) on the I2C bus.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Chassis/System Management (Critical)

SNMP Trap ID
mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0131

User Response
Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.
2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.
4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **5002070E : Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.**

The specified node is not able to communicate with the Chassis Management Module (CMM) on the I2C bus.

Severity
Error

Serviceable
Yes

Automatically notify support
Yes

Alert Category
Chassis/System Management (Critical)

SNMP Trap ID
mmTrapChassisC

CIM Information
Prefix: CMM **ID:** 0131

User Response
Complete the following steps until the problem is solved:

1. If more than one node is having this problem, reset the CMM, or fail over the CMM to the standby CMM if two CMMs are installed.

2. Check the event logs and any status indicators for the node for possible additional information about the problem. Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.
3. Perform a hard restart of the node system-management processor.
4. Perform a virtual reseat of the node. Attention: A virtual reseat shuts down power to the node. Check the interfaces of applications that are running to make sure that the node can be shut down safely.

- **66000701 : The CMM J40 jumper is installed in bay 1.**

  The J40 jumper is installed in the Chassis Management Module in CMM bay 1.

  Severity
  Warning

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0488

  User Response
  Remove the jumper.
- **66000702 : The CMM J40 jumper is installed in bay 2.**

  The J40 jumper is installed in the Chassis Management Module in CMM bay 2.

  Severity
  Warning

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Warning)

  SNMP Trap ID
  mmTrapChassisN

  CIM Information
  Prefix: CMM **ID:** 0489

  User Response
  Remove the jumper.
- **66000801 : The CMM J39 jumper is installed in bay 1.**

  The J39 jumper is installed in the Chassis Management Module in CMM bay 1.

  Severity

Warning

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0490

User Response
Remove the jumper.

- **66000802 : The CMM J39 jumper is installed in bay 2.**

The J39 jumper is installed in the Chassis Management Module in CMM bay 2.

Severity
Warning

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0491

User Response
Remove the jumper.

- **66000901 : Internal reset [arg1] of the CMM [arg2] software.**

The Chassis Management Module software encountered an unplanned reset. The software will automatically restart. Diagnostic information was collected in the service data.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information

Prefix: CMM **ID:** 0193

User Response
Information only; no action is required.

- **66000902 : Internal reset [arg1] of the CMM [arg2] software.**

The Chassis Management Module software encountered an unplanned reset. The software will automatically restart. Diagnostic information was collected in the service data.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0193

User Response
Information only; no action is required.

- **66000903 : The CMM 1 [arg1] [arg2] firmware image is corrupted. Unable to validate the signature.**

Security violation of image of CMM 1.

Severity
Warning

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0492

User Response
Reflash the code.

- **66000904 : The CMM 2 [arg1] [arg2] firmware image is corrupted. Unable to validate the signature.**

Security violation of image of CMM 2.

Severity
Warning

Serviceable
No

Automatically notify support

No

Alert Category
Chassis/System Management (Warning)

SNMP Trap ID
mmTrapChassisN

CIM Information
Prefix: CMM **ID:** 0493

User Response
Reflash the code.

- **6F100001 : Air filter service check is needed.**

The periodic air filter timer (reminder) has elapsed.

Severity
Informational

Serviceable
Yes

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0110

User Response
Complete the following steps:

1. Clean or replace the air filter, following the instructions in the Chassis Management Module Installation and Service Guide.
2. Reset the air filter service timer.

- **6F100100 : Air filter service timer was enabled to expire in [arg1] month(s) by user ID [arg2] from [arg3] at IP address [arg4].**

The specified user has enabled the air filter service reminder.

Severity
Informational

Serviceable
No

Automatically notify support
No

Alert Category
User activity (Informational)

SNMP Trap ID
mmTrapRemoteLoginS

CIM Information
Prefix: CMM **ID:** 0150

User Response
Information only; no action is required.

- **6F100200 : Air filter service timer was disabled by user ID [arg1] from [arg2] at IP address [arg3].**

  The specified user has disabled the air filter service reminder.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  User activity (Informational)

  SNMP Trap ID
  mmTrapRemoteLoginS

  CIM Information
  Prefix: CMM **ID:** 0227

  User Response
  Information only; no action is required.

- **6F609201 : Hardware inserted in [arg1].**

  Hardware has been installed in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0100

  User Response
  Information only; no action is required.

- **6F609202 : Hardware inserted in [arg1].**

  Hardware has been installed in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category

Inventory change (Informational)

SNMP Trap ID
mmTrapSysInvS

CIM Information
Prefix: CMM **ID:** 0100

User Response
Information only; no action is required.

- **6F609301 : Hardware removed from [arg1].**

  Hardware has been removed from the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0101

  User Response
  Information only; no action is required.

- **6F609302 : Hardware removed from [arg1].**

  Hardware has been removed from the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  Yes

  Automatically notify support
  No

  Alert Category
  Inventory change (Informational)

  SNMP Trap ID
  mmTrapSysInvS

  CIM Information
  Prefix: CMM **ID:** 0101

  User Response
  Information only; no action is required.

- **6F609401 : Discovered device [arg1] in [arg2], CRC: [arg3].**

  Hardware has been discovered successfully in the specified bay in the chassis.

  Severity
  Informational

Serviceable
No

Automatically notify support
No

Alert Category
Chassis/System Management (Informational)

SNMP Trap ID
mmTrapChassisS

CIM Information
Prefix: CMM **ID:** 0102

User Response
Information only; no action is required.

- **6F609402 : Discovered device [arg1] in [arg2], CRC: [arg3].**

  Hardware has been discovered successfully in the specified bay in the chassis.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0102

  User Response
  Information only; no action is required.

- **6F609501 : Failed to discover device [arg1] in [arg2].**

  Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0103

User Response
Information only; no action is required.

- **6F609502 : Failed to discover device [arg1] in [arg2].**

  Hardware has failed to be discovered in the specified bay in the chassis. This is normally raised when vital product data (VPD) could not be loaded or VPD failed CRC validation.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Chassis/System Management (Informational)

  SNMP Trap ID
  mmTrapChassisS

  CIM Information
  Prefix: CMM **ID:** 0103

  User Response
  Information only; no action is required.

- **77777701 : [arg1].**

  The system-management processor in the specified node has provided information to the Chassis Management Module (CMM). For more information about the issues that caused this message, view the system-event log of the node service interface. Event messages are documented in the information center and Installation and Service Guide for the node that is reporting the event.

  Severity
  Informational

  Serviceable
  No

  Automatically notify support
  No

  Alert Category
  Nodes (Informational)

  SNMP Trap ID
  mmTrapBladeS

  CIM Information
  Prefix: CMM **ID:** 0867

  User Response
  Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.

- **77777702 : [arg1].**

  The system-management processor in the specified node has provided information to the Chassis Management Module (CMM). For more information about the issues that caused this message, view the system-event log of the node service interface. Event messages are documented in the information center and Installation and Service Guide for the node that is reporting the event.

Severity
Warning

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
Prefix: CMM **ID:** 0868

User Response
Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.

- **77777703 : [arg1].**

The system-management processor in the specified node has provided information to the Chassis Management Module (CMM). For more information about the issues that caused this message, view the system-event log of the node service interface. Event messages are documented in the information center and Installation and Service Guide for the node that is reporting the event.

Severity
Error

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Critical)

SNMP Trap ID
mmTrapBladeC

CIM Information
Prefix: CMM **ID:** 0869

User Response
Follow the troubleshooting instructions in the information center or Installation and Service Guide for the node that is reporting the event. Check the documentation for any applications that are running for application-specific troubleshooting instructions.

CMM Events that automatically notify Support

You can configure the IBM Flex System Manager or the CMM to automatically notify Support (also known as *call home*) if certain types of errors are encountered. If you have configured this function, see the table for a list of events that automatically notify Support.

Table 10. Events that automatically notify Support

Event ID	Message String	Automatically Notify Support
00006011	The battery in Chassis Management Module [arg1] is low.	Yes
00006012	The battery in Chassis Management Module [arg1] is low.	Yes
00006120	Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.	Yes
00006121	Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.	Yes
00006122	Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.	Yes
00006123	Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.	Yes
00006124	Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.	Yes
00006125	Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.	Yes
00006126	Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.	Yes
00006220	Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.	Yes
00006221	Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.	Yes
00006222	Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.	Yes
00006223	Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.	Yes
00006224	Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.	Yes
00006225	Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.	Yes
00006226	Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.	Yes
00016802	Test call home by user ID [arg1] from [arg2] at IP address [arg3].	Yes
00016803	Manual call home generated by user ID [arg1] from [arg2] at IP address [arg3]. Message: [arg4].	Yes
00017104	CMM bay location cannot be determined, defaulting to CMM bay 2.	Yes
00022003	Primary Chassis Management Module real-time clock failed.	Yes
0002200A	Primary Chassis Management Module internal Ethernet logic failed.	Yes
00022015	Standby Chassis Management Module real-time clock failed.	Yes

Table 10. Events that automatically notify Support (continued)

Event ID	Message String	Automatically Notify Support
00022016	Standby Chassis Management Module local management bus failed.	Yes
00022019	Standby Chassis Management Module internal I/O logic failure.	Yes
0002201D	Standby Chassis Management Module internal Ethernet logic failed.	Yes
0002201E	Standby Chassis Management Module communication is offline.	Yes
0002205A	Primary Chassis Management Module internal I/O logic failure.	Yes
00026801	Fan module [arg1] has failed.	Yes
00026802	Fan module [arg1] has failed.	Yes
00026803	Fan module [arg1] has failed.	Yes
00026804	Fan module [arg1] has failed.	Yes
00026805	Fan module [arg1] has failed.	Yes
00026806	Fan module [arg1] has failed.	Yes
00026807	Fan module [arg1] has failed.	Yes
00026808	Fan module [arg1] has failed.	Yes
00026809	Fan module [arg1] has failed.	Yes
0002680A	Fan module [arg1] has failed.	Yes
00038201	Power supply [arg1] transient reading overvoltage.	Yes
00038202	Power supply [arg1] transient reading overvoltage.	Yes
00038203	Power supply [arg1] transient reading overvoltage.	Yes
00038204	Power supply [arg1] transient reading overvoltage.	Yes
00038205	Power supply [arg1] transient reading overvoltage.	Yes
00038206	Power supply [arg1] transient reading overvoltage.	Yes
00038301	Power supply [arg1] transient reading undervoltage.	Yes
00038302	Power supply [arg1] transient reading undervoltage.	Yes
00038303	Power supply [arg1] transient reading undervoltage.	Yes
00038304	Power supply [arg1] transient reading undervoltage.	Yes
00038305	Power supply [arg1] transient reading undervoltage.	Yes
00038306	Power supply [arg1] transient reading undervoltage.	Yes
00038401	Power supply [arg1] transient reading overcurrent.	Yes
00038402	Power supply [arg1] transient reading overcurrent.	Yes
00038403	Power supply [arg1] transient reading overcurrent.	Yes

Table 10. Events that automatically notify Support (continued)

Event ID	Message String	Automatically Notify Support
00038404	Power supply [arg1] transient reading overcurrent.	Yes
00038405	Power supply [arg1] transient reading overcurrent.	Yes
00038406	Power supply [arg1] transient reading overcurrent.	Yes
00038501	Power supply [arg1] power meter is offline.	Yes
00038502	Power supply [arg1] power meter is offline.	Yes
00038503	Power supply [arg1] power meter is offline.	Yes
00038504	Power supply [arg1] power meter is offline.	Yes
00038505	Power supply [arg1] power meter is offline.	Yes
00038506	Power supply [arg1] power meter is offline.	Yes
00038601	Fan module [arg1] VPD is not valid.	Yes
00038602	Fan module [arg1] VPD is not valid.	Yes
00038603	Fan module [arg1] VPD is not valid.	Yes
00038604	Fan module [arg1] VPD is not valid.	Yes
00038605	Fan module [arg1] VPD is not valid.	Yes
00038606	Fan module [arg1] VPD is not valid.	Yes
00038607	Fan module [arg1] VPD is not valid.	Yes
00038608	Fan module [arg1] VPD is not valid.	Yes
00038609	Fan module [arg1] VPD is not valid.	Yes
0003860A	Fan module [arg1] VPD is not valid.	Yes
00038701	Fan logic module [arg1] VPD is not valid.	Yes
00038702	Fan logic module [arg1] VPD is not valid.	Yes
00038A01	Power supply [arg1] VPD is not valid.	Yes
00038A02	Power supply [arg1] VPD is not valid.	Yes
00038A03	Power supply [arg1] VPD is not valid.	Yes
00038A04	Power supply [arg1] VPD is not valid.	Yes
00038A05	Power supply [arg1] VPD is not valid.	Yes
00038A06	Power supply [arg1] VPD is not valid.	Yes
00038F01	Internal proprietary management protocol between I/O module [arg1] and CMM is offline.	Yes
00038F02	Internal proprietary management protocol between I/O module [arg1] and CMM is offline.	Yes
00038F03	Internal proprietary management protocol between I/O module [arg1] and CMM is offline.	Yes
00038F04	Internal proprietary management protocol between I/O module [arg1] and CMM is offline.	Yes

Table 10. Events that automatically notify Support (continued)

Event ID	Message String	Automatically Notify Support
00039601	Fan module [arg1] VPD is not available.	Yes
00039602	Fan module [arg1] VPD is not available.	Yes
00039603	Fan module [arg1] VPD is not available.	Yes
00039604	Fan module [arg1] VPD is not available.	Yes
00039605	Fan module [arg1] VPD is not available.	Yes
00039606	Fan module [arg1] VPD is not available.	Yes
00039607	Fan module [arg1] VPD is not available.	Yes
00039608	Fan module [arg1] VPD is not available.	Yes
00039609	Fan module [arg1] VPD is not available.	Yes
0003960A	Fan module [arg1] VPD is not available.	Yes
00039701	Fan logic module [arg1] VPD is not available.	Yes
00039702	Fan logic module [arg1] VPD is not available.	Yes
00039A01	Power supply [arg1] VPD is not available.	Yes
00039A02	Power supply [arg1] VPD is not available.	Yes
00039A03	Power supply [arg1] VPD is not available.	Yes
00039A04	Power supply [arg1] VPD is not available.	Yes
00039A05	Power supply [arg1] VPD is not available.	Yes
00039A06	Power supply [arg1] VPD is not available.	Yes
00039B01	Fan module [arg1] fan parameter in VPD is not valid.	Yes
00039B02	Fan module [arg1] fan parameter in VPD is not valid.	Yes
00039B03	Fan module [arg1] fan parameter in VPD is not valid.	Yes
00039B04	Fan module [arg1] fan parameter in VPD is not valid.	Yes
00039B05	Fan module [arg1] fan parameter in VPD is not valid.	Yes
00039B06	Fan module [arg1] fan parameter in VPD is not valid.	Yes
00039B07	Fan module [arg1] fan parameter in VPD is not valid.	Yes
00039B08	Fan module [arg1] fan parameter in VPD is not valid.	Yes
00039B09	Fan module [arg1] fan parameter in VPD is not valid.	Yes
00039B0A	Fan module [arg1] fan parameter in VPD is not valid.	Yes
000A2101	Fan logic module [arg1] has failed.	Yes
000A2102	Fan logic module [arg1] has failed.	Yes
000A2201	Fan logic module [arg1] is an older revision card (FRU 81Y2912) and needs to be replaced.	Yes
000A2202	Fan logic module [arg1] is an older revision card (FRU 81Y2912) and needs to be replaced.	Yes

Table 10. Events that automatically notify Support (continued)

Event ID	Message String	Automatically Notify Support
000A6001	Fan module [arg1] is operating in a degraded state.	Yes
000A6002	Fan module [arg1] is operating in a degraded state.	Yes
000A6003	Fan module [arg1] is operating in a degraded state.	Yes
000A6004	Fan module [arg1] is operating in a degraded state.	Yes
000A6005	Fan module [arg1] is operating in a degraded state.	Yes
000A6006	Fan module [arg1] is operating in a degraded state.	Yes
000A6007	Fan module [arg1] is operating in a degraded state.	Yes
000A6008	Fan module [arg1] is operating in a degraded state.	Yes
000A6009	Fan module [arg1] is operating in a degraded state.	Yes
000A600A	Fan module [arg1] is operating in a degraded state.	Yes
08028001	Power supply [arg1] is off. DC fault.	Yes
08028002	Power supply [arg1] is off. DC fault.	Yes
08028003	Power supply [arg1] is off. DC fault.	Yes
08028004	Power supply [arg1] is off. DC fault.	Yes
08028005	Power supply [arg1] is off. DC fault.	Yes
08028006	Power supply [arg1] is off. DC fault.	Yes
08200001	Power supply [arg1] communication is offline.	Yes
08200002	Power supply [arg1] communication is offline.	Yes
08200003	Power supply [arg1] communication is offline.	Yes
08200004	Power supply [arg1] communication is offline.	Yes
08200005	Power supply [arg1] communication is offline.	Yes
08200006	Power supply [arg1] communication is offline.	Yes
08216301	Mismatched power supplies in the chassis: [arg1]. The configuration is not supported.	Yes
08236001	Power supply [arg1] has shut down because of an overcurrent fault.	Yes
08236002	Power supply [arg1] has shut down because of an overcurrent fault.	Yes
08236003	Power supply [arg1] has shut down because of an overcurrent fault.	Yes
08236004	Power supply [arg1] has shut down because of an overcurrent fault.	Yes
08236005	Power supply [arg1] has shut down because of an overcurrent fault.	Yes
08236006	Power supply [arg1] has shut down because of an overcurrent fault.	Yes

Table 10. Events that automatically notify Support (continued)

Event ID	Message String	Automatically Notify Support
08236481	Power supply [arg1] has shut down because of an overvoltage fault.	Yes
08236482	Power supply [arg1] has shut down because of an overvoltage fault.	Yes
08236483	Power supply [arg1] has shut down because of an overvoltage fault.	Yes
08236484	Power supply [arg1] has shut down because of an overvoltage fault.	Yes
08236485	Power supply [arg1] has shut down because of an overvoltage fault.	Yes
08236486	Power supply [arg1] has shut down because of an overvoltage fault.	Yes
08236801	Power supply [arg1] has shut down because of an undervoltage fault.	Yes
08236802	Power supply [arg1] has shut down because of an undervoltage fault.	Yes
08236803	Power supply [arg1] has shut down because of an undervoltage fault.	Yes
08236804	Power supply [arg1] has shut down because of an undervoltage fault.	Yes
08236805	Power supply [arg1] has shut down because of an undervoltage fault.	Yes
08236806	Power supply [arg1] has shut down because of an undervoltage fault.	Yes
08526001	Power supply [arg1] encountered an internal fan failure.	Yes
08526002	Power supply [arg1] encountered an internal fan failure.	Yes
08526003	Power supply [arg1] encountered an internal fan failure.	Yes
08526004	Power supply [arg1] encountered an internal fan failure.	Yes
08526005	Power supply [arg1] encountered an internal fan failure.	Yes
08526006	Power supply [arg1] encountered an internal fan failure.	Yes
08556001	An internal fan in power supply [arg1] is operating outside the recommended speed.	Yes
08556002	An internal fan in power supply [arg1] is operating outside the recommended speed.	Yes
08556003	An internal fan in power supply [arg1] is operating outside the recommended speed.	Yes
08556004	An internal fan in power supply [arg1] is operating outside the recommended speed.	Yes
08556005	An internal fan in power supply [arg1] is operating outside the recommended speed.	Yes

Table 10. Events that automatically notify Support (continued)

Event ID	Message String	Automatically Notify Support
08556006	An internal fan in power supply [arg1] is operating outside the recommended speed.	Yes
0901E000	Chassis front LED card not present.	Yes
0901E003	Chassis rear LED card not present.	Yes
0E010001	Node [arg1] device [arg2][[arg3]] VPD is not available.	Yes
0E010002	Node [arg1] device [arg2][[arg3]] VPD is not available.	Yes
0E010003	Node [arg1] device [arg2][[arg3]] VPD is not available.	Yes
0E010004	Node [arg1] device [arg2][[arg3]] VPD is not available.	Yes
0E010005	Node [arg1] device [arg2][[arg3]] VPD is not available.	Yes
0E010006	Node [arg1] device [arg2][[arg3]] VPD is not available.	Yes
0E010007	Node [arg1] device [arg2][[arg3]] VPD is not available.	Yes
0E010008	Node [arg1] device [arg2][[arg3]] VPD is not available.	Yes
0E010009	Node [arg1] device [arg2][[arg3]] VPD is not available.	Yes
0E01000A	Node [arg1] device [arg2][[arg3]] VPD is not available.	Yes
0E01000B	Node [arg1] device [arg2][[arg3]] VPD is not available.	Yes
0E01000C	Node [arg1] device [arg2][[arg3]] VPD is not available.	Yes
0E01000D	Node [arg1] device [arg2][[arg3]] VPD is not available.	Yes
0E01000E	Node [arg1] device [arg2][[arg3]] VPD is not available.	Yes
0EA00001	I/O module [arg1] fault.	Yes
0EA00002	I/O module [arg1] fault.	Yes
0EA00003	I/O module [arg1] fault.	Yes
0EA00004	I/O module [arg1] fault.	Yes
0EA1A401	I/O module [arg1] current fault.	Yes
0EA1A402	I/O module [arg1] current fault.	Yes
0EA1A403	I/O module [arg1] current fault.	Yes
0EA1A404	I/O module [arg1] current fault.	Yes
0EA1F801	I/O module [arg1] communication failure.	Yes
0EA1F802	I/O module [arg1] communication failure.	Yes
0EA1F803	I/O module [arg1] communication failure.	Yes
0EA1F804	I/O module [arg1] communication failure.	Yes
0EA2D001	The internal proprietary management credentials for [arg1] are incorrect with error code: [arg2].	Yes
0EA2D002	The internal proprietary management credentials for [arg1] are incorrect with error code: [arg2].	Yes

Table 10. Events that automatically notify Support (continued)

Event ID	Message String	Automatically Notify Support
0EA2D003	The internal proprietary management credentials for [arg1] are incorrect with error code: [arg2].	Yes
0EA2D004	The internal proprietary management credentials for [arg1] are incorrect with error code: [arg2].	Yes
35010481	Node [arg1] device [arg2][[arg3]] VPD is not valid.	Yes
35010482	Node [arg1] device [arg2][[arg3]] VPD is not valid.	Yes
35010483	Node [arg1] device [arg2][[arg3]] VPD is not valid.	Yes
35010484	Node [arg1] device [arg2][[arg3]] VPD is not valid.	Yes
35010485	Node [arg1] device [arg2][[arg3]] VPD is not valid.	Yes
35010486	Node [arg1] device [arg2][[arg3]] VPD is not valid.	Yes
35010487	Node [arg1] device [arg2][[arg3]] VPD is not valid.	Yes
35010488	Node [arg1] device [arg2][[arg3]] VPD is not valid.	Yes
35010489	Node [arg1] device [arg2][[arg3]] VPD is not valid.	Yes
3501048A	Node [arg1] device [arg2][[arg3]] VPD is not valid.	Yes
3501048B	Node [arg1] device [arg2][[arg3]] VPD is not valid.	Yes
3501048C	Node [arg1] device [arg2][[arg3]] VPD is not valid.	Yes
3501048D	Node [arg1] device [arg2][[arg3]] VPD is not valid.	Yes
3501048E	Node [arg1] device [arg2][[arg3]] VPD is not valid.	Yes
35010801	Unexpected exception affecting [arg1] was encountered in security service.	Yes
35010802	Unexpected exception affecting [arg1] was encountered in security service.	Yes
35010803	Unexpected exception affecting [arg1] was encountered in security service.	Yes
35010804	Unexpected exception affecting [arg1] was encountered in security service.	Yes
35010805	Unexpected exception affecting [arg1] was encountered in security service.	Yes
35010806	Unexpected exception affecting [arg1] was encountered in security service.	Yes
35010807	Unexpected exception affecting [arg1] was encountered in security service.	Yes
35010808	Unexpected exception affecting [arg1] was encountered in security service.	Yes
35010809	Unexpected exception affecting [arg1] was encountered in security service.	Yes
3501080A	Unexpected exception affecting [arg1] was encountered in security service.	Yes

Table 10. Events that automatically notify Support (continued)

Event ID	Message String	Automatically Notify Support
3501080B	Unexpected exception affecting [arg1] was encountered in security service.	Yes
3501080C	Unexpected exception affecting [arg1] was encountered in security service.	Yes
3501080D	Unexpected exception affecting [arg1] was encountered in security service.	Yes
3501080E	Unexpected exception affecting [arg1] was encountered in security service.	Yes
35010841	Unexpected exception was encountered in security service or system-management processor on [arg1].	Yes
35010842	Unexpected exception was encountered in security service or system-management processor on [arg1].	Yes
35010843	Unexpected exception was encountered in security service or system-management processor on [arg1].	Yes
35010844	Unexpected exception was encountered in security service or system-management processor on [arg1].	Yes
35010845	Unexpected exception was encountered in security service or system-management processor on [arg1].	Yes
35010846	Unexpected exception was encountered in security service or system-management processor on [arg1].	Yes
35010847	Unexpected exception was encountered in security service or system-management processor on [arg1].	Yes
35010848	Unexpected exception was encountered in security service or system-management processor on [arg1].	Yes
35010849	Unexpected exception was encountered in security service or system-management processor on [arg1].	Yes
3501084A	Unexpected exception was encountered in security service or system-management processor on [arg1].	Yes
3501084B	Unexpected exception was encountered in security service or system-management processor on [arg1].	Yes
3501084C	Unexpected exception was encountered in security service or system-management processor on [arg1].	Yes
3501084D	Unexpected exception was encountered in security service or system-management processor on [arg1].	Yes
3501084E	Unexpected exception was encountered in security service or system-management processor on [arg1].	Yes
35010A00	Chassis Management Module configuration is not compliant with the security policy.	Yes
4001711E	Standby Chassis Management Module failed to synchronize with the primary CMM. Standby network interface is disabled.	Yes
40040000	Chassis VPD is not valid.	Yes

Table 10. Events that automatically notify Support (continued)

Event ID	Message String	Automatically Notify Support
40040001	Chassis VPD is not available.	Yes
40040101	I/O module [arg1] VPD is not valid.	Yes
40040102	I/O module [arg1] VPD is not valid.	Yes
40040103	I/O module [arg1] VPD is not valid.	Yes
40040104	I/O module [arg1] VPD is not valid.	Yes
40040201	Chassis Management Module [arg1] VPD is not valid.	Yes
40040202	Chassis Management Module [arg1] VPD is not valid.	Yes
40040401	Chassis Management Module [arg1] VPD is not available.	Yes
40040402	Chassis Management Module [arg1] VPD is not available.	Yes
40040501	Chassis Management Module [arg1] is not compatible. Redundant capability is turned off.	Yes
40040502	Chassis Management Module [arg1] is not compatible. Redundant capability is turned off.	Yes
50020000	Not reading device on system management (I2C) bus [arg1]. Chassis Management Module in the chassis [arg2] communication is offline.	Yes
50020101	Not reading device on system management (I2C) bus [arg1]. The rear LED card in the chassis [arg2] communication is offline.	Yes
50020102	Not reading device on system management (I2C) bus [arg1]. The rear LED card in the chassis [arg2] communication is offline.	Yes
50020201	Not reading device on system management (I2C) bus [arg1]. Fan logic module [arg2] communication is offline.	Yes
50020202	Not reading device on system management (I2C) bus [arg1]. Fan logic module [arg2] communication is offline.	Yes
50020281	Not reading device on system management (I2C) bus [arg1]. Fan logic module [arg2] VPD communication is offline.	Yes
50020282	Not reading device on system management (I2C) bus [arg1]. Fan logic module [arg2] VPD communication is offline.	Yes
50020301	Not reading device on system management (I2C) bus [arg1]. I/O module [arg2] communication is offline.	Yes
50020302	Not reading device on system management (I2C) bus [arg1]. I/O module [arg2] communication is offline.	Yes
50020303	Not reading device on system management (I2C) bus [arg1]. I/O module [arg2] communication is offline.	Yes
50020304	Not reading device on system management (I2C) bus [arg1]. I/O module [arg2] communication is offline.	Yes
50020401	Not reading device on system management (I2C) bus [arg1]. Fan module [arg2] communication is offline.	Yes

Table 10. Events that automatically notify Support (continued)

Event ID	Message String	Automatically Notify Support
50020402	Not reading device on system management (I2C) bus [arg1]. Fan module [arg2] communication is offline.	Yes
50020403	Not reading device on system management (I2C) bus [arg1]. Fan module [arg2] communication is offline.	Yes
50020404	Not reading device on system management (I2C) bus [arg1]. Fan module [arg2] communication is offline.	Yes
50020405	Not reading device on system management (I2C) bus [arg1]. Fan module [arg2] communication is offline.	Yes
50020406	Not reading device on system management (I2C) bus [arg1]. Fan module [arg2] communication is offline.	Yes
50020407	Not reading device on system management (I2C) bus [arg1]. Fan module [arg2] communication is offline.	Yes
50020408	Not reading device on system management (I2C) bus [arg1]. Fan module [arg2] communication is offline.	Yes
50020409	Not reading device on system management (I2C) bus [arg1]. Fan module [arg2] communication is offline.	Yes
5002040A	Not reading device on system management (I2C) bus [arg1]. Fan module [arg2] communication is offline.	Yes
50020501	Not reading device on system management (I2C) bus [arg1]. Power supply [arg2] communication is offline.	Yes
50020502	Not reading device on system management (I2C) bus [arg1]. Power supply [arg2] communication is offline.	Yes
50020503	Not reading device on system management (I2C) bus [arg1]. Power supply [arg2] communication is offline.	Yes
50020504	Not reading device on system management (I2C) bus [arg1]. Power supply [arg2] communication is offline.	Yes
50020505	Not reading device on system management (I2C) bus [arg1]. Power supply [arg2] communication is offline.	Yes
50020506	Not reading device on system management (I2C) bus [arg1]. Power supply [arg2] communication is offline.	Yes
50020601	Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.	Yes
50020602	Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.	Yes
50020603	Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.	Yes
50020604	Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.	Yes
50020605	Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.	Yes
50020606	Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.	Yes

Table 10. Events that automatically notify Support (continued)

Event ID	Message String	Automatically Notify Support
50020607	Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.	Yes
50020608	Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.	Yes
50020609	Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.	Yes
5002060A	Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.	Yes
5002060B	Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.	Yes
5002060C	Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.	Yes
5002060D	Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.	Yes
5002060E	Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.	Yes
50020701	Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.	Yes
50020702	Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.	Yes
50020703	Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.	Yes
50020704	Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.	Yes
50020705	Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.	Yes
50020706	Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.	Yes
50020707	Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.	Yes
50020708	Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.	Yes
50020709	Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.	Yes
5002070A	Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.	Yes
5002070B	Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.	Yes
5002070C	Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.	Yes

Table 10. Events that automatically notify Support (continued)

Event ID	Message String	Automatically Notify Support
5002070D	Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.	Yes
5002070E	Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.	Yes

Lenovo XClarity Administrator alerts and events

If a Lenovo XClarity Administrator is available, system alerts and events for all monitored endpoints are displayed in an event log.

The Lenovo XClarity Administrator provides a list of serviceable alerts and an event log:

- Alerts are hardware or management conditions that need investigation and user action. The Lenovo XClarity Administrator polls the managed endpoints asynchronously and displays alerts received from those endpoints. When an alert is received, a corresponding event is stored in the event log. It is possible to have an alert without a corresponding event in the event log.
- The event log provides a historical list of all hardware and management events.

See http://flexsystem.lenovofiles.com/help/topic/com.lenovo.lxca.doc/aug_product_page.html for more information about working with alerts and events.

Flex System Manager event log

If an Flex System Manager management node is installed, event codes and corrective actions for all monitored chassis and nodes are displayed in the management node event log.

The Flex System Manager management node event log contains a filtered subset of integrated management module (IMM) events, unified extensible firmware interface (UEFI) events, Chassis Management Module (CMM) events, and system management interrupt (SMI) events.

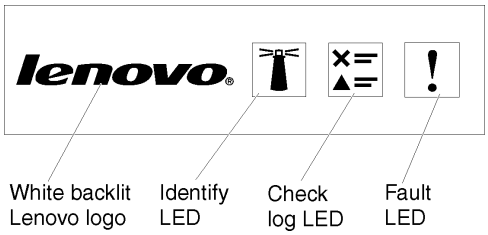
- The integrated management module in each compute node monitors the node and posts events in the node IMM event log. These events are also sent to the CMM event log and to the Flex System Manager event log, if a management node is installed.
- Event codes for the management node are displayed in the management node IMM event log and in the Flex System Manager event log.

You can view the Flex System Manager event log through the web interface. See http://flexsystem.lenovofiles.com/help/index.jsp for more information about viewing the Flex System Manager event log.

Front information panel LEDs

LEDs are displayed on the front information panel and on the rear of the Flex System Enterprise Chassis.

The following illustration shows the LEDs on the front information panel. The Identify, Check log, and Fault LEDs on the front information panel are also visible on the rear of the chassis.

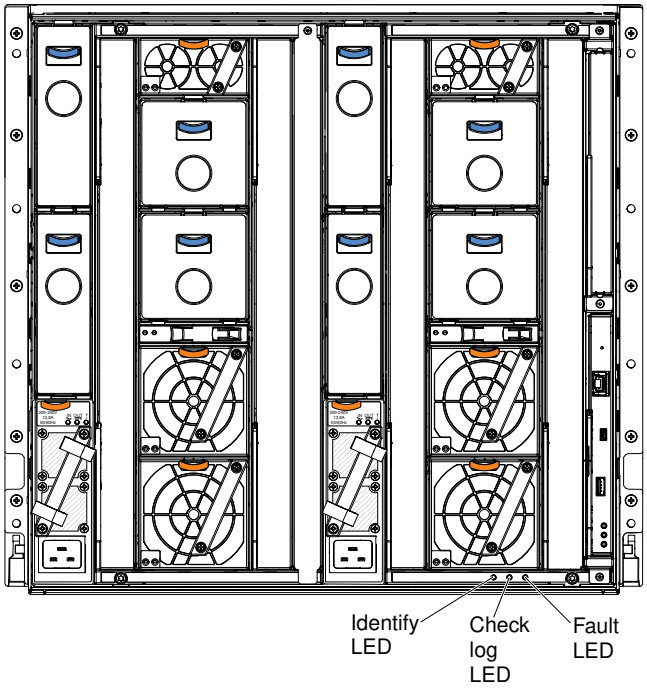


The system front information panel LEDs table is a three-column table that describes the LEDs located on the chassis front information panel. Column 1 identifies the LEDs. Column 2 describes the function of the LED. Column 3 describes the user actions needed to correct faults, if indicated.

LED	Description	Action
Backlit logo	When the logo is lit, the chassis has power.	If the logo is not lit and the system has power, if a Flex System Manager management node is installed, check the event log from the management node; otherwise, check for active events in the Chassis Management Module web interface.
Identify	The system administrator can remotely light this blue LED to aid in visually locating the chassis. When this LED is lit or flashing, it indicates the location of the chassis, or it indicates that the Chassis Management Module has detected a condition in the chassis that requires attention.	If the LED is lit, if a Flex System Manager management node is installed, check the event log from the management node; otherwise, check for active events in the Chassis Management Module web interface.
Check log	When this yellow LED is lit, it indicates that an error has occurred but has not been isolated. Check the event logs.	
Fault	When this yellow LED is lit, it indicates that a hardware error has occurred. Check the event logs.	

Chassis rear information panel LEDs

The following illustration shows the location of the information panel LEDs that are visible on the rear of the Flex System Enterprise Chassis.



The chassis rear information panel LEDs table is a three-column table that describes the LEDs located on the chassis rear information panel. Column 1 identifies the LEDs. Column 2 describes the function of the LED. Column 3 describes the user actions needed to correct faults, if indicated.

LED	Description	Action
Identify	The system administrator can remotely light this blue LED to aid in visually locating the chassis. When this LED is lit or flashing, it indicates the location of the chassis, or it indicates that the Chassis Management Module has detected a condition in the chassis that requires attention.	If the LED is lit, if a Flex System Manager management node is installed, check the event log from the management node; otherwise, check for active events in the Chassis Management Module web interface.
Check log	When this yellow LED is lit, it indicates that an error has occurred but has not been isolated. Check the event logs.	
Fault	When this yellow LED is lit, it indicates that a hardware error has occurred. Check the event logs.	

Chassis module LEDs

Each module contains LEDs that can be used to isolate failed components.

Note: To find descriptions and actions for LEDs on I/O modules or compute nodes, see the documentation that comes with the device. You can find the documentation for I/O modules at http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.networkdevices.doc/network.html and for compute nodes at http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.common.nav.doc/compute_blades.html.

The chassis module LEDs table is a three-column table that describes the function of the LEDs on each chassis module. Column 1 identifies the LEDs. Column 2 describes the normal and fault states of the LED. Column 3 describes the user actions needed to correct faults, if indicated.

Module name/LED	Description	User action
Chassis management module		
Fault LED	This yellow LED is lit when an error has occurred in the CMM. The system fault LED on the chassis will also be lit.	If this LED is lit, check the Flex System Manager event log for CMM-related errors and follow the corrective actions for those events.
Flex System Manager		
Fault LED	This yellow LED is lit when an error has occurred in the Flex System Manager. The system fault LED on the chassis will also be lit.	If this LED is lit, check the Flex System Manager event log for Flex System Manager-related errors and follow the corrective actions for those events. See the *Flex System Manager Installation and Service Guide* for more information.
Power supply		
AC power LED	This green LED is **not** lit if there is an ac power problem.	If this LED is **not** lit, check the Flex System Manager event log, if installed, or the CMM event log for power-related errors and follow the corrective actions for those events.
DC power LED	The green LED is **not** lit if there is an dc power problem.	If this LED is **not** lit, check the Flex System Manager event log, if installed, or the CMM event log for power-related errors and follow the corrective actions for those events.
Fault LED	This yellow LED is lit if the power supply has failed.	If this LED is lit, check the Flex System Manager event log, if installed, or the CMM event log for power-related errors and follow the corrective actions for those events.
Fan module		
Fault LED	This yellow LED is lit if one of the fans in the fan module has failed. **Note:** If one of the fans in the fan module fails, the other fan will begin operating at full speed.	If this LED is lit, check the Flex System Manager event log, if installed, or the CMM event log for fan-related errors and follow the corrective actions for those events.
Fan logic module		
Fault LED	This yellow LED is lit if one of the fan logic modules fail.	If this LED is lit, check the Flex System Manager event log, if installed, or the CMM event log for fan-related errors and follow the corrective actions for those events. .

Troubleshooting by symptom

Use the information in this section to troubleshoot observable problems in the chassis.

Troubleshoot the chassis by symptom when there is limited event code information or when there are observable problems that are not reflected in the event logs.

To troubleshoot a compute node by symptom, see the documentation that comes with the compute node. Compute node documentation is available from http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.common.nav.doc/compute_blades.html.

See “Network integration with the Flex System Manager” on page 52 for diagrams of the chassis management and data networks.

Cannot communicate with the Flex System Manager management node

Use the information in this section to troubleshoot the chassis when you cannot communicate with the Flex System Manager management node.

Action

Complete the following steps until the problem is solved:

1. Make sure that the correct ports in the connection path are enabled and that you can ping the management node. If you are unable to ping the management node, see “Cannot ping the Flex System Manager management node on the data network” on page 935 for more information.
2. Make sure that the protocols that you are using are enabled.

   Note: By default, only secure protocols are enabled, for example, SSH and HTTPS.
3. If you cannot log into the management node, see “Cannot log in to the Flex System Manager management node” on page 931.

Cannot communicate with the CMM

Use the information in this section to troubleshoot the chassis when you cannot communicate with the CMM on the data network.

Action

Complete the following steps until the problem is solved:

1. Make sure that the correct ports in the connection path are enabled and that you can ping the CMM. If you are unable to ping the CMM, see “Cannot ping the CMM on the management network” on page 931 for more information.
2. Make sure that the protocols that you are using are enabled.

   Note: By default, only secure protocols are enabled, for example, SSH and HTTPS.
3. Make sure that you can log into the CMM. If you are unable to log into the CMM, see “Cannot log in to the CMM” on page 931.
4. Reset the CMM to the default settings by pressing the reset button on the CMM.

Note: You must press and hold the CMM reset button for at least 10 seconds to reset the CMM to default settings. All user-modified CMM configuration settings will be reset to the factory default value.

Cannot communicate with the I/O module

Use the information in this section to troubleshoot the chassis when you cannot communicate with the I/O module.

Action

Complete the following steps until the problem is solved:

1. Make sure that the correct ports in the connection path are enabled and that you can ping the I/O module. If you are unable to ping the I/O module, see “Cannot ping the I/O module” on page 933 for more information.
2. Make sure that the protocols that you are using are enabled.

   Note: By default, only secure protocols are enabled, for example, SSH and HTTPS.

3. Make sure that you can log into the I/O module. If you are unable to log into the I/O module, see “Cannot log in to the I/O module” on page 931.
4. Use a serial cable to connect to the I/O module to further isolate the problem.

Cannot log in

Use the information in this section to troubleshoot the chassis when you cannot log in to the management node, the CMM, or the I/O module.

Cannot log in to the Flex System Manager management node

Use the information in this section to troubleshoot the chassis when you cannot log in to the management node.

Action

Complete the following steps until the problem is solved:

1. Make sure that you are using the correct password and that the capitals lock is off.
2. Contact Lenovo Support for further assistance if you have forgotten the password.

Cannot log in to the CMM

Use the information in this section to troubleshoot the chassis when you cannot log in to the CMM.

Action

Complete the following steps until the problem is solved:

1. Make sure that you are using the correct password and that the capitals lock is off.
2. If you have forgotten the password, restore the CMM default settings by pressing the reset button on the CMM.

Cannot log in to the I/O module

Use the information in this section to troubleshoot the chassis when you cannot log in to the I/O module.

Action

Complete the following steps until the problem is solved:

1. Make sure that you are using the correct password and that the capitals lock is off.
2. Connect a serial cable to the I/O module to further isolate the problem.
3. If you have forgotten the password, restore the I/O module to default settings.

Cannot ping the CMM on the management network

Use the information in this section to troubleshoot the chassis when one or more compute nodes cannot ping the CMM on the management network.

See “Network integration with the Flex System Manager” on page 52 for a diagram of the chassis management network.

Single node cannot ping the CMM in the same chassis

Use the information in this section to troubleshoot a single node that cannot ping the CMM on the management network in the same chassis.

Action

Complete the following steps until the problem is solved:

1. Make sure that the Chassis Management Module is powered on and the applicable ports are enabled on the CMM.
2. Make sure that the compute node IMM has acquired an IP address from the CMM by using the Setup utility on the node.

   Note: If the CMM recently lost connection to the DCHP server, you must reset the IMM by using the CMM interface so that a new IP address can be acquired.
3. In the CMM user interface, click **Chassis Management > Component IP Configuration** and make sure that the IP address that is listed is the same as the IP address that is displayed in the Setup utility. If it is not the same IP address, configure the IMM network settings correctly or reset the IMM to automatically acquire a new IP address.
4. Check http://support.lenovo.com for any firmware updates that might apply to this problem. You can view the release notes for a firmware update to determine the issues that the update addresses.
5. Remove the compute node from the chassis and check the connectors on the back of the node for bent pins. If the pins are bent, contact Support.
6. Install the compute node in another node bay to determine whether the problem remains. If the problem remains, make sure that the compute node is connected to a port that has been enabled and that the vLAN settings allow that port to connect to the network.
7. Check http://support.lenovo.com for any service bulletins that are related to network connectivity.
8. (Trained service technician only) Complete the following steps:
   a. Force the link/duplex speed.
   b. Check the connectors on the I/O module to make sure that no pins are bent.
   c. Check the connectors on the chassis midplane to make sure that no pins are bent.
   d. Remove the CMM and install a working CMM in the same bay.
      - If the problem is solved, replace the CMM that you removed.
      - If the problem remains, replace the chassis midplane.

Multiple nodes cannot ping the CMM in the same chassis

Use the information in this section to troubleshoot multiple nodes that cannot ping the CMM on the management network in the same chassis.

Action

Complete the following steps until the problem is solved:

1. Make sure that the Chassis Management Module is powered on and the applicable ports are enabled on the CMM. If the CMM is hung, reset the CMM.
2. Reset the CMM.
3. Check for firmware updates for the CMM.
4. Reset the CMM to factory defaults and attempt to discover the nodes again. Allow enough time for the IMMs to acquire a network address.
5. Replace the CMM.
6. Make sure that the compute node IMM has acquired an IP address from the CMM by using the Setup utility on the node.

   Note: If the CMM recently lost connection to the DCHP server, you must reset the IMM by using the CMM interface so that a new IP address can be acquired.
7. In the CMM user interface, click **Chassis Management > Component IP Configuration** and make sure that the IP address that is listed is the same as the IP address that is displayed in the Setup utility. If it is

not the same IP address, configure the IMM network settings correctly or reset the IMM to automatically acquire a new IP address.

8. Check http://support.lenovo.com for any firmware updates that might apply to this problem. You can view the release notes for a firmware update to determine the issues that the update addresses.
9. Remove the compute node from the chassis and check the connectors on the back of the node for bent pins. If the pins are bent, contact Support.
10. Check http://support.lenovo.com for any service bulletins that are related to network connectivity.
11. (Trained service technician only) Complete the following steps:
    a. Force the link/duplex speed.
    b. Check the connectors on the CMM to make sure that no pins are bent.
    c. Check the connectors on the chassis midplane to make sure that no pins are bent.
    d. Remove the CMM and install a working CMM in the same bay.
        - If the problem is solved, replace the CMM that you removed.

CMM cannot ping the CMM in a different chassis

Use the information in this section to troubleshoot a CMM that cannot ping the CMM in a different chassis.

Action

Complete the following steps until the problem is solved:

1. Make sure that the Chassis Management Modules are powered on and the applicable ports are enabled.
    a. If the CMM is powered on and hung, reset the CMM.
    b. Make sure that the IMM, the management node, and the CMMs are all on the same subnet.
2. Verify that the cables between the CMMs and the top-of-rack switch are correctly connected and that the activity LEDs are lit on the applicable ports. Make sure that the applicable ports are enabled in the I/O module.
3. If you are using a DHCP server for the management network, make sure that the CMM is configured correctly.
4. Connect the CMM to a different port on the top-of-rack switch. Make sure that the activity LEDs are lit on the port and that the port is enabled.
5. Check http://support.lenovo.com for any firmware updates that might apply to this problem. You can view the release notes for a firmware update to determine the issues that the update addresses.
6. Check http://support.lenovo.com for any service bulletins that are related to network connectivity.
7. (Trained service technician only) Complete the following steps:
    a. Force the link/duplex speed.
    b. Check the connectors on the CMM and on the chassis midplane to make sure that no pins are bent.
    c. Replace the CMM that cannot connect to the network.

Cannot ping the I/O module

Use the information in this section to troubleshoot the chassis when one or more compute nodes cannot ping the I/O module.

See “Network integration with the Flex System Manager” on page 52 for diagrams of the chassis management and data networks.

Single node cannot ping the I/O module

Use the information in this section to troubleshoot a single node that cannot ping the I/O module.

Action

Complete the following steps until the problem is solved:

1. If you have recently updated the firmware for one or more devices in the chassis (I/O module) and have verified the network settings, install the previous level of firmware.
2. Make sure that the I/O module is powered on and the applicable ports are enabled on the I/O module.
3. Make sure that all network cables are correctly connected and that the activity LEDs are lit. If the cables are correctly connected and the LEDs are not lit, replace the cable.
4. Check http://support.lenovo.com for any firmware updates that might apply to this problem. You can view the release notes for a firmware update to determine the issues that are addressed by the update.
5. Remove the node from the chassis and check the connectors at the back of the node for bent pins. If the pins are bent, go to http://support.lenovo.com to submit a service request.
6. Install the compute node in another node bay, if one is available. If the problem remains, make sure that the compute node is connected to a port that has been enabled and that the vLAN settings allow that port to connect to the network.
7. Check http://support.lenovo.com for any service bulletins that are related to I/O-module connectivity.
8. If the problem remains, replace the I/O module, and go to http://support.lenovo.com to submit a service request.
9. (Trained service technician only) Complete the following steps:
   a. Force the link/duplex speed.
   b. Check the connectors on the I/O module to make sure that no pins are bent.
   c. Check the connectors on the chassis midplane to make sure that no pins are bent.
   d. Remove the I/O module and install a working I/O module in the same I/O bay.
      - If the problem is solved, replace the I/O module that you removed.

Multiple nodes cannot ping the I/O module

Use the information in this section to troubleshoot multiple nodes that cannot ping the I/O module.

Action

Complete the following steps until the problem is solved:

1. If you have recently updated the firmware for one or more devices in the chassis (I/O module or CMM), install the previous level of firmware.
2. Make sure that the I/O module is powered on and the applicable ports are enabled on the I/O module.
3. Make sure that all network cables are correctly connected and that the activity LEDs are lit.
4. From the compute node operating system, verify that the network device is active. Check also the network settings, such as IP address, subnet mask (if you are using IPv4), DNS, DHCP settings, and vLAN settings to make sure that the settings match the settings of the network device. See the documentation that comes with the operating system for information about viewing network devices and checking the network settings.
5. Check http://support.lenovo.com for any firmware updates that might apply to this problem. You can view the release notes for a firmware update to determine the issues that are addressed by the update.
6. Check http://support.lenovo.com for any service bulletins that are related to network connectivity.
7. (Trained service technician only) Complete the following steps:
   a. Force the link/duplex speed.
   b. Check the connectors on the I/O module to make sure that no pins are bent.
   c. Check the connectors on the chassis midplane to make sure that no pins are bent.

d. Remove the I/O module and install a working I/O module in the same I/O bay.
   - If the problem is solved, replace the I/O module that you removed.

Cannot ping the Flex System Manager management node on the data network

Use the information in this section to troubleshoot the chassis when one or more compute nodes cannot ping the management node on the data network.

See "Network integration with the Flex System Manager" on page 52 for a diagram of the chassis data network.

Single node cannot ping the management node in the same chassis

Use the information in this section to troubleshoot a single node that cannot ping the Flex System Manager management node in the same chassis on the data network.

Action

Complete the following steps until the problem is solved:

1. Make sure that the management node is powered on and is not hung, by logging in to the management node. If you are unable to log in from the management network, attempt to log in from the data network. If the management node is powered on and hung, perform a virtual reseat of the management node from the CMM.
2. Make sure that the I/O module is powered on and is not hung, by pinging the I/O module from the management node. If the I/O module is powered on and hung, reset the I/O module. Make sure that the correct ports are enabled for the node on the I/O module. Also make sure that all of the network cables in the communication path are correctly connected.
3. Make sure that the compute node is the only one in the chassis that cannot ping the management node. If it is not, follow the steps in "Multiple nodes cannot ping the management node in the same chassis" on page 936.
4. Make sure that the configuration settings in the node are correct and that the port is enabled.
5. Check http://support.lenovo.com for any firmware updates that might apply to this issue. You can view the release notes for a firmware update to determine the issues that are addressed by the update.
6. Check http://support.lenovo.com for any service bulletins that are related to network connectivity.
7. Remove the compute node and make sure that the connectors on the midplane and the node are not damaged.
8. (Trained service technician only) Complete the following steps:
   a. Force the link/duplex speed.
   b. Check the connectors on the node and the midplane to make sure that no pins are bent.

Single node cannot ping the management node in a different chassis

Use the information in this section to troubleshoot a single node that cannot ping the Flex System Manager management node in a different chassis on the data network.

Action

Complete the following steps until the problem is solved:

1. Make sure that the management node is powered on and is not hung, by logging in to the management node. If you are unable to log in from the management network, attempt to log in from the data network. If the management node is powered on and hung, perform a virtual reseat of the management node from the CMM.

2. Make sure that the I/O module is powered on and is not hung, by pinging the I/O module from the management node. If the I/O module is powered on and hung, reset the I/O module. Make sure that the correct ports are enabled for the node on the I/O module. Also make sure that all of the network cables in the communication path are correctly connected.
3. Make sure that the compute node is the only one in the chassis that cannot ping the management node. If it is not, follow the steps in "Multiple nodes cannot ping the management node in the same chassis" on page 936.
4. Make sure that the IP configuration settings on the node are correct and that the port is enabled.
5. Check http://support.lenovo.com for any firmware updates that might apply to this issue. You can view the release notes for a firmware update to determine the issues that are addressed by the update.
6. Check http://support.lenovo.com for any service bulletins that are related to network connectivity.
7. Remove the compute node and make sure that the connectors on the midplane and the node are not damaged.
8. (Trained service technician only) Complete the following steps:
   a. Force the link/duplex speed.
   b. Check the connectors on the node and the midplane to make sure that no pins are bent.

Multiple nodes cannot ping the management node in the same chassis

Use the information in this section to troubleshoot multiple nodes that cannot ping the Flex System Manager management node in the same chassis on the data network.

Action

Complete the following steps until the problem is solved:

1. Make sure that the management node is powered on and is not hung, by logging in to the management node. If you are unable to log in from the management network, attempt to log in from the data network. If the management node is powered on and hung, perform a virtual reseat of the management node from the CMM.
2. Make sure that the I/O module is powered on and is not hung, by pinging the I/O module from the management node. If the I/O module is powered on and hung, reset the I/O module. Make sure that the correct ports are enabled for the node on the I/O module. Also make sure that all of the network cables in the communication path are correctly connected.
3. Make sure that the management network port (eth1) is enabled in the management node. Make sure that the port configuration settings are correct for the data network.
4. Make sure that the configuration settings for each node are correct and that the data network ports are enabled.
5. Make sure that the configuration settings in the I/O module are correct and that the appropriate ports are enabled for your compute nodes and the management node on the I/O module. If the problem remains, complete the following steps:
   a. Restart the I/O module.
   b. Check http://support.lenovo.com for any firmware updates that might apply to this issue. You can view the release notes for a firmware update to determine the issues that are addressed by the update.
   c. Perform a virtual reseat of the I/O module.
   d. Replace the I/O module.
6. Check http://support.lenovo.com for any service bulletins that are related to network connectivity.
7. Remove the management node and make sure that the connectors on the chassis midplane and the management node are not damaged.

8. (Trained service technician only) Complete the following steps:
   a. Force the link/duplex speed.
   b. Check the connectors on the nodes and the chassis midplane to make sure that no pins are bent.
   c. Replace the I/O expansion card in the management node.

Multiple nodes cannot ping the management node in a different chassis

Use the information in this section to troubleshoot multiple nodes that cannot ping the Flex System Manager management node in a different chassis on the data network.

Action

Complete the following steps until the problem is solved:

1. Make sure that the management node is powered on and is not hung, by logging in to the management node. If you are unable to log in from the management network, attempt to log in from the data network. If the management node is powered on and hung, perform a virtual reseat of the management node from the CMM.
2. Make sure that the I/O module is powered on and is not hung, by pinging the I/O module from the management node. If the I/O module is powered on and hung, reset the I/O module. Make sure that the correct ports are enabled for the node on the I/O module. Also make sure that all of the network cables in the communication path are correctly connected.
3. Make sure that the management network port (eth1) in the management node is enabled. Make sure that the port configuration settings are correct for the data network.
4. Make sure that the configuration settings for each node are correct and that the data network ports are enabled.
5. Make sure that the configuration settings in the I/O module are correct and that the applicable ports are enabled for your compute nodes and the management node on the I/O module. If the problem remains, complete the following steps:
   a. Restart the I/O module.
   b. Check http://support.lenovo.com for any firmware updates that might apply to this issue. You can view the release notes for a firmware update to determine the issues that are addressed by the update.
   c. Perform a virtual reseat of the I/O module.
   d. Replace the I/O module.
6. Check http://support.lenovo.com for any service bulletins that are related to network connectivity.
7. Remove the management node and make sure that the connectors on the chassis midplane and the node are not damaged.
8. (Trained service technician only) Complete the following steps:
   a. Force the link/duplex speed.
   b. Check the connectors on the nodes and the chassis midplane to make sure that no pins are bent.
   c. Replace the I/O expansion card in the management node.

Multiple nodes cannot ping the management node in the same chassis or a different chassis

Use the information in this section to troubleshoot multiple nodes that cannot ping the Flex System Manager management node in the same chassis or a different chassis on the data network.

Action

Complete the following steps until the problem is solved:

1. Follow the steps in “Multiple nodes cannot ping the management node in the same chassis” on page 936.
2. Follow the steps in “Multiple nodes cannot ping the management node in a different chassis” on page 937.

Cannot ping the Flex System Manager management node on the management network

Use the information in this section to troubleshoot the chassis when one or more compute nodes cannot ping the management node on the management network.

See “Network integration with the Flex System Manager” on page 52 for a diagram of the chassis management network.

Single node cannot ping the management node in the same chassis

Use the information in this section to troubleshoot a single node that cannot ping the Flex System Manager management node in the same chassis on the management network.

Action

Complete the following steps until the problem is solved:

1. Make sure that the management node is powered on and is not hung, by logging in to the management node. If you are unable to log in from the management network, attempt to log in from the data network. If the management node is powered on and hung, perform a virtual reseat of the management node from the CMM.
2. Make sure that the CMM is powered on and is not hung, by pinging the CMM from the management node. If the CMM is powered on and hung, reset the CMM. Make sure that the IMM, the management node, and CMM are all on the same subnet.
3. Make sure that the compute node is the only one in the chassis that the management node cannot ping. If it is not, follow the steps in “Multiple nodes cannot ping the management node in the same chassis” on page 939. Make sure that the compute node appears on the chassis map (it might not be fully discovered by the management node software).
4. Make sure that the system-management processor in each compute node has a valid IP address by checking the chassis map of the remote chassis.

   Note: If the CMM recently lost connection to the DCHP server, you must reset the IMM by using the CMM interface so that a new IP address can be acquired.
5. In the CMM user interface, click **Chassis Management > Component IP Configuration** and make sure that the IP address that is listed is the same as the IP address that is displayed in the Setup utility. If it is not the same, configure the IMM network settings correctly.
6. Check http://support.lenovo.com for any firmware updates that might apply to this issue. You can view the release notes for a firmware update to determine the issues that are addressed by the update.
7. Check http://support.lenovo.com for any service bulletins that are related to network connectivity.
8. Remove the compute node and make sure that the connectors on the chassis midplane and the node are not damaged.
9. (Trained service technician only) Complete the following steps:
   a. Force the link/duplex speed.
   b. Check the connectors on the node and the chassis midplane to make sure that no pins are bent.
   c. Replace the system-board assembly.

Single node cannot ping the management node in a different chassis

Use the information in this section to troubleshoot a single node that cannot ping the Flex System Manager management node in a different chassis on the management network.

Action

Complete the following steps until the problem is solved:

1. Make sure that the management node is powered on and is not hung, by logging in to the management node. If you are unable to log in from the management network, attempt to log in from the data network. If the management node is powered on and hung, perform a virtual reseat of the management node from the CMM.
2. Make sure that all of the network cables in the communication path are correctly connected.
3. Make sure that the CMM is powered on and is not hung, by pinging the CMM from the management node:
   a. If the CMM is powered on and hung, reset the CMM
   b. Make sure that the IMM, the management node, and CMM are all on the same subnet.
4. Make sure that the compute node is the only one in the chassis that cannot ping the management node. If it is not, follow the steps in "Multiple nodes cannot ping the management node in the same chassis" on page 939. Make sure that the compute node appears on the chassis map (it might not be fully discovered by the management node software).
5. Make sure that the IMM has acquired an IP address from the CMM by using the Setup utility on the compute node.

   Note: If the CMM recently lost connection to the DCHP server, you must reset the IMM by using the CMM interface so that a new IP address can be acquired.
6. Make sure that the system-management processor in each compute node has a valid IP address by checking the chassis map of the remote chassis.

   Note: If the CMM recently lost connection to the DCHP server, you must reset the IMM by using the CMM interface so that a new IP address can be acquired.
7. Check http://support.lenovo.com for any firmware updates that might apply to this issue. You can view the release notes for a firmware update to determine the issues that are addressed by the update.
8. Check http://support.lenovo.com for any service bulletins that are related to network connectivity.
9. Remove the compute node and make sure that the connectors on the chassis midplane and the node are not damaged.
10. (Trained service technician only) Complete the following step:
    a. Check the connectors on the node and the chassis midplane to make sure that no pins are bent.

Multiple nodes cannot ping the management node in the same chassis

Use the information in this section to troubleshoot multiple nodes that cannot ping the Flex System Manager management node in the same chassis on the management network.

Action

Complete the following steps until the problem is solved:

1. Make sure that the management node is powered on and is not hung, by logging in to the management node. If you are unable to log in from the management network, attempt to log in from the data network. If the management node is powered on and hung, perform a virtual reseat of the management node from the CMM.
2. Make sure that the CMM is powered on and is not hung, by pinging the CMM from the management node:

a. If the CMM is powered on and hung, reset the CMM.

b. Make sure that the IMM, the management node, and CMM are all on the same subnet.

3. Make sure that the management network port (eth0) in the management node is enabled.
4. Make sure that the management node has an IP address, is on the same subnet as the CMM, and is able to ping the CMM.
5. Make sure that the system-management processor in each compute node has a valid IP address by checking the chassis map of the remote chassis.

   Note: If the CMM recently lost connection to the DCHP server, you must reset the IMM by using the CMM interface so that a new IP address can be acquired.

   If a system-management processor does not have a valid IP address, complete the following steps:

   a. Restart the CMM.

   b. Check http://support.lenovo.com for any firmware or software updates that might apply to this issue. You can view the release notes for a firmware update to determine the issues that are addressed by the update.

   c. Remove and reinstall CMM.

   d. Replace the CMM.
6. Check http://support.lenovo.com for any service bulletins that are related to network connectivity.
7. Remove the management node and make sure that the connectors on the chassis midplane and the management node are not damaged.
8. (Trained service technician only) Complete the following steps:

   a. Force the link/duplex speed.

   b. Check the connectors on the nodes and the chassis midplane to make sure that no pins are bent.

   c. Replace the I/O expansion card in the management node.

Multiple nodes cannot ping the management node in a different chassis

Use the information in this section to troubleshoot multiple nodes that cannot ping the Flex System Manager management node in a different chassis on the management network.

Action

Complete the following steps until the problem is solved:

1. Make sure that the management node is powered on and is not hung, by logging in to the management node. If you are unable to log in from the management network, attempt to log in from the data network. If the management node is powered on and hung, perform a virtual reseat of the management node from the CMM.
2. Make sure that all of the network cables in the communication path are correctly connected.
3. Make sure that the CMMs (the CMM in the same chassis as the management node and the CMM in the remote chassis) are powered on and are not hung by pinging the CMM from the management node:

   a. If the CMM is powered on and hung, reset the CMM.

   b. Make sure that the IMM, the management node, and the CMM are all on the same subnet.
4. Make sure that all cables between the CMMs and the top-of-rack switch are correctly connected and secure and that the activity LEDs are lit on the applicable ports
5. Make sure that the CMMs (the CMM in the same chassis as the management node and the CMM in the remote chassis) have the same subnet address and can ping one another. If they cannot, make sure that the ports on the top-of-rack switch are enabled. Attempt to connect the CMMs directly if possible.

6. Make sure that the management node has fully discovered the nodes within its chassis by viewing the chassis map. If it has not fully discovered the nodes, follow the steps in "Multiple nodes cannot ping the management node in the same chassis" on page 939.
7. Make sure that the management processor for each compute node has a valid IP address by checking the chassis map of the remote chassis.

   Note: If the CMM recently lost connection to the DCHP server, you must reset the IMM by using the CMM interface so that a new IP address can be acquired.

   If a system-management processor does not have a valid IP address, complete the following steps:

   a. Restart the CMM in the remote chassis.
   b. Check http://support.lenovo.com for any firmware or software updates that might apply to this issue. You can view the release notes for a firmware update to determine the issues that are addressed by the update.
   c. Remove and reinstall the CMM.
   d. Replace the CMM.
8. Check http://support.lenovo.com for any service bulletins that are related to network connectivity.
9. Remove the node and make sure that the connectors on the chassis midplane and the node are not damaged.
10. (Trained service technician only) Complete the following steps:
    a. Force the link/duplex speed.
    b. Check the connectors on the nodes and the chassis midplane to make sure that no pins are bent.
    c. Replace the I/O expansion card in the management node.

Multiple nodes cannot ping the management node in the same chassis or a different chassis

Use the information in this section to troubleshoot multiple nodes that cannot ping the Flex System Manager management node in the same chassis or a different chassis on the management network.

Action

Complete the following steps until the problem is solved:

1. Make sure that all of the network cables in the communication path are correctly connected.
2. Follow the steps in "Multiple nodes cannot ping the management node in the same chassis" on page 939.
3. Follow the steps in "Multiple nodes cannot ping the management node in a different chassis" on page 940.

Compute node connectivity problems

This section provides information about where to find the information to solve compute node problems.

For information about solving compute node connectivity problems, see the troubleshooting information in the compute node documentation. Compute node documentation is available from http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.common.nav.doc/compute_blades.html.

To determine which compute nodes are compatible with the Flex System Enterprise Chassis, see http://www.lenovo.com/serverproven/.

Intermittent connectivity problems

Use the information in this section to troubleshoot intermittent connectivity problems in the chassis.

Single node - loss of connectivity to the data network

Use the information in this section to troubleshoot intermittent single-node connectivity loss in the chassis.

Action

Complete the following steps until the problem is solved:

1. Make sure that the network cables are correctly connected in the ports of the I/O module and that the I/O module is correctly seated.
2. Update the device driver for the node that is related to the NIC or for the storage device controller.
3. Check the I/O-module documentation for information about solving connectivity problems.

Multiple nodes - loss of connectivity to the data network

Use the information in this section to troubleshoot intermittent multiple-node connectivity loss in the chassis.

Action

Complete the following steps until the problem is solved:

1. Test the I/O module that the devices are connected to by using the diagnostic tools that are provided by the manufacturer.
2. Attempt to connect one node to the network first, and then try to bring the others online to isolate the problem.
3. Check the I/O module firmware and update it if necessary.

   Important: Rebooting and running POST diagnostics on the I/O module might also help to isolate the problem; however, this will temporarily disable the data network.

Multiple nodes cannot connect

Use the information in this section to troubleshoot the chassis when multiple nodes cannot connect to the network.

Multiple nodes cannot connect to the data network during initial setup

Use the information in this section to troubleshoot the chassis when multiple nodes cannot connect to the network during initial setup.

Action

Complete the following steps until the problem is solved:

1. If you have just updated the firmware for one or more devices in the chassis (such as an I/O module or Chassis Management Module), install the previous level of firmware.
2. Make sure that the I/O module is powered on and the applicable ports are enabled on the I/O module.
3. Verify that all cables between the I/O module and the network device (switch or router) are correctly connected and secure and that the activity LEDs are lit on the applicable ports.
4. From the compute node operating system, verify that the network device is active. See the documentation that comes with the operating system for information about viewing network devices. From the compute node operating system, check the network settings, such as IP address, subnet mask (if you are using IPv4), DNS, DHCP settings, and vLAN settings, to make sure that the settings match the settings of the network device. See the documentation that comes with the operating system for information about checking network settings.

5. Check http://support.lenovo.com for any firmware updates that might apply to this problem. You can view the release notes for a firmware update to determine the issues that the update addresses.
6. Check http://support.lenovo.com for any service bulletins that are related to network connectivity.
7. (Trained service technician only) Complete the following steps:
   a. Force the link/duplex speed.
   b. Check the connectors on the I/O module to make sure that no pins are bent.
   c. Check the connectors on the chassis midplane to make sure that no pins are bent.
   d. Remove the I/O module and install a working I/O module in the same I/O bay. If the problem is solved, replace the I/O module that you removed.

Sudden connectivity loss to multiple nodes

This section describes how to troubleshoot sudden connectivity loss to multiple nodes.

Action

Perform this step to resolve the problem:

1. If there is a sudden loss of connectivity for multiple nodes, the event should be logged in the event logs. See the event log for the Flex System Manager management node, if installed, or see the Chassis Management Module event log to determine what actions might be required to resolve this problem.

Node power problems

Use the information in this section to troubleshoot compute nodes that will not power on or will not power off.

Single node will not power on

Use the information in this section to troubleshoot a single-node that will not power on.

Action

Complete the following steps until the problem is solved:

1. Check the event logs for any events that are related to the compute node, and solve them. If an Flex System Manager management node is installed, check the event log on the management node. Otherwise, check the event log on the Chassis Management Module.
2. Make sure that the CMM can recognize the compute node. Log in to the CMM user interface and verify that the compute node appears in the chassis view. If the CMM cannot recognize the compute node, remove the compute node and inspect the compute node and the back of the node bay to make sure there is no physical damage to the connectors.
3. Make sure that the power management policy that is implemented on the CMM is sufficient to enable the compute node to power on.

   Note: For more information about setting the CMM power management policy, see Setting the CMM power management policies"Setting the CMM power management policies" in the *Flex System Chassis Management Module User's Guide*.
4. Make sure that the Flex System Manager management node has completed the discovery of the compute node. Log in to the Flex System Manager user interface and verify that the compute node appears in the chassis view from the CMM.
5. Replace the system-board assembly.

   Note: Until you are able to replace the system-board assembly, you can attempt to power on the compute node from the CMM or from the Flex System Manager user interface.

Multiple nodes will not power on

Use the information in this section to troubleshoot multiple nodes that will not power on.

Action

1. Check the event logs for any events that are related to the compute nodes, and solve them. If an Flex System Manager management node is installed, check the event log on the management node. Otherwise, check the event log on the Chassis Management Module.
2. Make sure that the power management policy that is implemented on the CMM is sufficient to enable the compute nodes to power on.

   Note: For more information about setting the CMM power management policy, see Setting the CMM power management policies"Setting the CMM power management policies" in the *Flex System Chassis Management Module User's Guide*.

Compute node will not power off

Use the information in this section to troubleshoot a compute node that will not power off.

Action

Complete the following steps until the problem is solved:

1. Attempt to power off the compute node through the Flex System Manager user interface, if a Flex System Manager management node is installed. Otherwise, attempt to power off the compute node through the CMM user interface.
2. Attempt to restart the system-management processor for the compute node. You can restart the system-management processor through the CMM user interface. Click the compute node in the chassis view and then click **Restart System Mgmt Processor**. After the system-management processor has been restarted, attempt to power off the compute node from the CMM.
3. Attempt to power off the compute node by using the power button on the front of the node.
4. Attempt to reset the compute node from the CMM command-line interface (CLI) by using the `reset` command.
5. Reseat the CMM; then, perform steps 1-4 again.

Overheating

Use the information in this section to troubleshoot nodes or chassis that might be overheating.

Multiple nodes or chassis overheating

Use the information in this section to troubleshoot multiple nodes or chassis that might be overheating.

Action

Complete the following steps until the problem is solved:

1. Verify that the room where the system is located is properly cooled.
2. Check the event logs for rising temperature events and fan module events. If a Flex System Manager management node is installed, check the event log on the management node. Otherwise, check the event log on the Chassis Management Module. If there are no rising temperature or fan module events, the node is running within normal operating temperatures.

   Note: Some variation in operating temperature is to be expected.

Single node overheating

Use the information in this section to troubleshoot a single node that might be overheating.

Action

Check the event logs for rising temperature events and fan module events. If a Flex System Manager management node is installed, check the event log on the management node. Otherwise, check the event log on the Chassis Management Module. If there are no rising temperature events, the node is running within normal operating temperatures.

Note: Some variation in operating temperature is to be expected.

Poor network performance

Use the information in this section to troubleshoot network performance problems, for example, slow response time.

Action

Complete the following steps until the problem is solved:

1. Isolate the network (such as storage, data, or management) that is operating slowly. Use ping tools or operating-system tools such as a task manager or resource manager to isolate the network.
2. Check for traffic congestion on the network.
3. Update the device driver for the node that is related to the NIC or for the storage device controller.
4. Use the traffic diagnostic tools that are provided by your I/O module manufacturer.

Power supply problems

Use the information in this section to troubleshoot a power supply problem.

Action

Complete the following steps until the problem is solved:

1. Check the CMM event log or the Flex System Manager event log, if one is installed, and resolve any issues pertaining to the power supply.
2. Make sure that the CMM power management policy is set correctly.

   Note: For more information about setting the CMM power management policy, see Setting the CMM power management policies"Setting the CMM power management policies" in the *Flex System Chassis Management Module User's Guide*.
3. Check the status of the In, Out and Fault lights on the power supply:
   - If the In light is not lit, make sure that the outlet it is connected to is powered and that the power cord is functional.
   - If the In light remains off, replace the power supply.
   - If the Out light is off, unplug the power cord for a few seconds, then reconnect it. If the problem persists, replace the power supply.
   - If the Fault light is on, unplug the power cord for a few seconds, then reconnect it. If the problem persists, replace the power supply.

Single node cannot ping the I/O module

Use the information in this section to troubleshoot a single node that cannot ping the I/O module.

Action

Complete the following steps until the problem is solved:

1. If you have recently updated the firmware for one or more devices in the chassis (I/O module) and have verified the network settings, install the previous level of firmware.
2. Make sure that the I/O module is powered on and the applicable ports are enabled on the I/O module.
3. Make sure that all network cables are correctly connected and that the activity LEDs are lit. If the cables are correctly connected and the LEDs are not lit, replace the cable.
4. Check http://support.lenovo.com for any firmware updates that might apply to this problem. You can view the release notes for a firmware update to determine the issues that are addressed by the update.
5. Remove the node from the chassis and check the connectors at the back of the node for bent pins. If the pins are bent, go to http://support.lenovo.com to submit a service request.
6. Install the compute node in another node bay, if one is available. If the problem remains, make sure that the compute node is connected to a port that has been enabled and that the vLAN settings allow that port to connect to the network.
7. Check http://support.lenovo.com for any service bulletins that are related to I/O-module connectivity.
8. If the problem remains, replace the I/O module, and go to http://support.lenovo.com to submit a service request.
9. (Trained service technician only) Complete the following steps:
   a. Force the link/duplex speed.
   b. Check the connectors on the I/O module to make sure that no pins are bent.
   c. Check the connectors on the chassis midplane to make sure that no pins are bent.
   d. Remove the I/O module and install a working I/O module in the same I/O bay.
      - If the problem is solved, replace the I/O module that you removed.

Unusual noises coming from a power supply or fan module

Use the information in this section to troubleshoot unusual noises from a power supply or fan module.

During normal operation, the chassis fan modules and power supplies might be loud, and the chassis fan modules might temporarily run at full speed. If you detect unusual noises from the chassis that are not part of normal operation, use this information to isolate the problem.

Squealing, scratching, grinding, or groaning noises

Use the information in this section to troubleshoot squealing, scratching, grinding, or groaning noises from a power supply or fan module.

Action

Remove the power supplies and fan modules one at a time. If the noise stops, replace the power supply or fan module that you just removed.

Note: When you remove and replace the power supplies and fan modules, these events will be displayed in the event logs.

Jet or fast-moving air noises

Use the information in this section to troubleshoot jet or fast-moving air noises from a power supply or fan module.

Action

Check the event logs for events that are related to high temperatures or a failed fan module. These events can cause the fan speed to increase to make sure that the chassis is cooled properly. In addition, you might notice an increased noise from the power-supply fans.

Clicking or rattling noises

Use the information in this section to troubleshoot clicking or rattling noises from a power supply or fan module.

Action

Complete the following steps until the problem is solved:

1. Visually inspect the fan modules and power-supply fans to make sure that nothing (such as a wire or a broken fan blade) is touching the fan blades.

   Important: If an object is touching or rubbing against a fan blade, be sure to shut down the chassis before you attempt to remove the object.

2. Remove the fan modules and power supplies one at a time. If the noise stops, replace the fan module or power supply that you just removed.

Unusual odors

Use the information in this section to troubleshoot unusual odors from the chassis.

Action

If you have just installed a new component, the odor might be from the new component. Otherwise, go to http://support.lenovo.com and submit a service request.

Visible physical damage

This section describes what to do if the chassis or components have visible physical damage.

Action

Perform these steps to solve the problem:

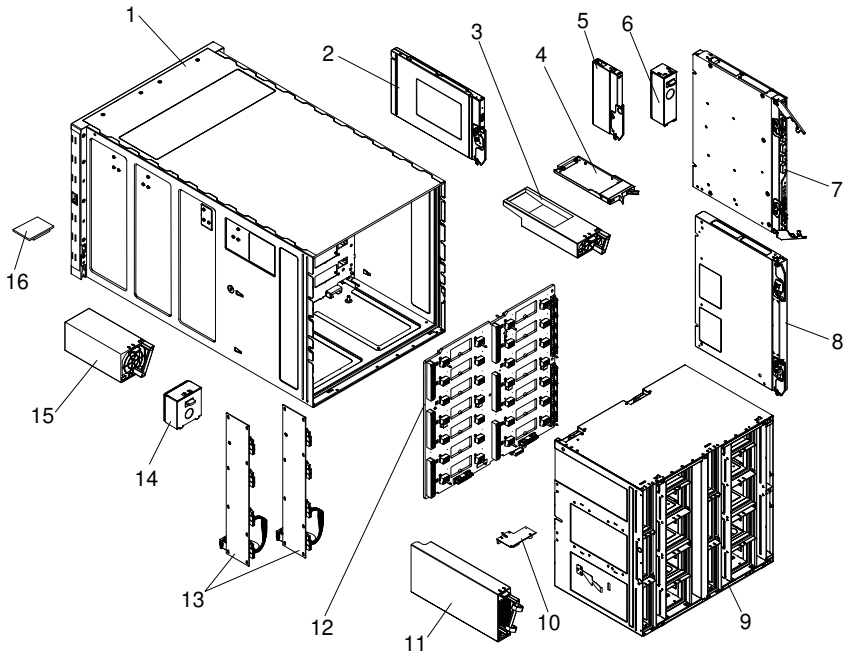
1. Go to http://support.lenovo.com and submit a service request if you have a chassis, component, or node that appears to be physically damaged.

Chapter 5. Parts listing, Types 7893, 8721, and 8724

Use this information to locate and identify replaceable components that are available for the Flex System Enterprise Chassis.

For an updated parts listing go to http://support.lenovo.com and search for `systemserviceparts`.

Note: The illustrations in this document might differ slightly from your hardware.



Replaceable components consist of consumable parts, structural parts, field replaceable units (FRUs), and customer replaceable units (CRUs):

- **Consumable parts:** Purchase and replacement of consumable parts (components, such as batteries and printer cartridges, that have depletable life) is your responsibility. If Lenovo acquires or installs a consumable component at your request, you will be charged for the service.
- **Structural parts:** Purchase and replacement of structural parts (components, such as chassis shell, bay fillers, and bezel) is your responsibility. If Lenovo acquires or installs a structural component at your request, you will be charged for the service.
- **Field replaceable unit (FRU):** FRUs must be replaced only by a trained service technician, unless they are classified as customer replaceable units (CRUs).
- **Tier 1 customer replaceable unit (CRU):** Replacement of Tier 1 CRUs is your responsibility. If Lenovo installs a Tier 1 CRU at your request without a service contract, you will be charged for the installation.
- **Tier 2 customer replaceable unit:** You may install a Tier 2 CRU yourself or request Lenovo to install it, at no additional charge, under the type of warranty service that is designated for your Flex System Enterprise Chassis.

For information about the terms of the warranty, see the *Warranty Information* document that comes with the Flex System Enterprise Chassis.

Index	Description	CRU part number (Tier 1)	CRU part number (Tier 2)	FRU part number
2	Lenovo Flex System Chassis Management Module (models A1x, DCx, FT1 and HC1)	00AN232		
2	Lenovo Flex System Chassis Management Module 2 (models ALx, DLx, FT2 and HC2)	00FG678 or 01PF404		
3	Fan module, 40 mm	81Y2911		
4	Fan logic module	94Y5805		
7	I/O module [1]	Note 1		
9	Shuttle (with card and cable assembly)			81Y2892
10	LED card, rear			Comes with midplane FRU. See item 12.
11	2100 W power supply, 200 - 240 V ac, C20 connector [2]	94Y8253 or 69Y5892		
11	2500 W power supply	94Y8251 or 69Y5890		
11	2500 W power supply	94Y8307 or 94Y8303		
11	2500 W HVDC power supply, 240 - 380 V dc, RF-203 connector [2]	94Y8274		
11	2500 W -48 V power supply, -48 to -60 V dc, 2 position power connector [2]	94Y8265 or 94Y8296		
11	2500 W power supply	00YJ921		
11	2500 W power supply	01PF561		
11	2500 W power supply	00MX939, 01PF526, 01PF551 or 00MX920		
11	2100 W power supply	00YJ917 or 00MX926		
11	2500 W power supply	00YJ931 or 00YJ910		
11	2500 W power supply	94Y8281		
11	2500 W power supply	03HC904		
12	Midplane and rear LED card (models A1x, DCx, FT1 and HC1)			81Y2893
12	Midplane and rear LED card (models ALx, DLx, FT2 and HC2)			00MP727
13	Fan distribution card			81Y2980
15	Dual rotor fan module, 80 mm	81Y2910 or 02YF966		
16	LED card, front			81Y2901
	Battery, 3.0 V (Chassis Management Module)	33F8354		

Index	Description	CRU part number (Tier 1)	CRU part number (Tier 2)	FRU part number
	Chassis cable kit, includes the following cables: • Cable, rear LED card to front LED card • Cable, 40 mm fan module to fan distribution card • Cable, fan logic module to fan distribution card		49Y4993	
	Console breakout cable	81Y2889 or 02JJ069		
	Damper, node bay		81Y2904	
	Serial cable, mini USB to RJ45 (FC9340)	90Y9340		
	Serial cable, mini USB to DB9 (FC0510)	43X0510		
	Lenovo 40G Base QSFP+ bi-directional transceiver	00YL675		
	NE2552E Flex Switch	01KN246		
	25-GB Base-SR Ethernet transceiver module	00YD275		
	100-GB Base-SR4 Ethernet transceiver module	00YD277		
	100-GB Base-LR4 Ethernet transceiver module	00YD278		
	Fiber adapter panel (FAP) active optical cable (AOC), 3M 25G	00YD279		
	Fiber adapter panel (FAP) active optical cable (AOC), 5M 25G	00YD280		
	Fiber adapter panel (FAP) active optical cable (AOC), 10M 25G	00YD281		
	Fiber adapter panel (FAP) active optical cable (AOC), 15M 25G	00YD282		
	Fiber adapter panel (FAP) active optical cable (AOC), 20M 25G	00YD283		
	Fiber adapter panel (FAP) active optical cable (AOC), 3M 100G	00YD284		
	Fiber adapter panel (FAP) active optical cable (AOC), 5M 100G	00YD285		
	Fiber adapter panel (FAP) active optical cable (AOC), 10M 100G	00YD286		
	Fiber adapter panel (FAP) active optical cable (AOC), 15M 100G	00YD287		
	Fiber adapter panel (FAP) active optical cable (AOC), 20M 100G	00YD288		
	Fiber adapter panel (FAP) active optical cable (AOC), 3M 100G to 4x25G	00YD289		
	Fiber adapter panel (FAP) active optical cable (AOC), 5M 100G to 4x25G	00YD290		

Index	Description	CRU part number (Tier 1)	CRU part number (Tier 2)	FRU part number
	Fiber adapter panel (FAP) active optical cable (AOC), 10M 100G to 4x25G	00YD291		
	Fiber adapter panel (FAP) active optical cable (AOC), 15M 100G to 4x25G	00YD292		
	Fiber adapter panel (FAP) active optical cable (AOC), 20M 100G to 4x25G	00YD293		
	Fiber adapter panel (FAP) direct attach cable (DAC), 1M 25G	00YD295		
	Fiber adapter panel (FAP) direct attach cable (DAC), 3M 25G	00YD296		
	Fiber adapter panel (FAP) direct attach cable (DAC), 5M 25G	00YD297		
	Fiber adapter panel (FAP) direct attach cable (DAC), 1M 100G	00YD299		
	Fiber adapter panel (FAP) direct attach cable (DAC), 3M 100G	01GV910		
	Fiber adapter panel (FAP) direct attach cable (DAC), 5M 100G	01GV911		
	Fiber adapter panel (FAP) direct attach cable (DAC), 1M 100G to 4x25G	01GV912		
	Fiber adapter panel (FAP) direct attach cable (DAC), 3M 100G to 4x25G	01GV913		
	Fiber adapter panel (FAP) direct attach cable (DAC), 5M 100G to 4x25G	01GV914		
	Fiber adapter panel (FAP) OM4 multimode fiber (MMF) cable, 5M	01GV915		
	Fiber adapter panel (FAP) OM4 multimode fiber (MMF) cable, 7M	01GV916		
	Fiber adapter panel (FAP) OM4 multimode fiber (MMF) cable, 10M	01GV917		
	Fiber adapter panel (FAP) OM4 multimode fiber (MMF) cable, 15M	01GV918		
	Fiber adapter panel (FAP) OM4 multimode fiber (MMF) cable, 20M	01GV919		
	Fiber adapter panel (FAP) OM4 multimode fiber (MMF) cable, 30M	01GV920		
	Fiber adapter panel (FAP) OM4 breakout cable, 1M	01GV921		
	Fiber adapter panel (FAP) OM4 breakout cable, 3M	01GV922		
	Fiber adapter panel (FAP) OM4 breakout cable, 5M	01GV923		
	Active optical cable (AOC), 1M 100G	01KN959		

Index	Description	CRU part number (Tier 1)	CRU part number (Tier 2)	FRU part number
	Cable, LWL 8G SFP+	00MY765		
	Cable, ELWL 8G SFP+	00MY767		
	100GBase-SR4 BiDi QSFP28 Transceiver	01PF054		
	SI4091 10Gb System Interconnect Module	00CG543		

1. See http://www.lenovo.com/serverproven/ for a list of the I/O modules that are compatible with the Flex System Enterprise Chassis.
2. Do not mix different types of power supplies. Each chassis must contain either all ac-powered supplies or all dc-powered supplies.
   - For ac-powered chassis, do not mix 2100 W and 2500 W power supplies. Chassis powered by ac power should contain only power supplies of the same wattage.
   - For dc-powered chassis, do not mix 240 to 380 V dc and -48 to -60 V dc power supplies. Chassis powered by dc power should contain only power supplies of the same input voltage.

Consumable and structural parts

Consumable and structural parts are not covered by the Statement of Limited Warranty.

Index	Description	Part number
1	Chassis shell (without shuttle)	81Y2891
5	Filler, CMM	81Y2898
6	Filler, power supply	81Y2896
8	Filler, I/O module	81Y2897
14	Filler, 80 mm fan module	81Y2899
	Airborne contaminant filter assembly (optional FC2908)	81Y2908
	Dust filter replacement pack for airborne contaminant filter assembly (4 filters)	43W9057
	Chassis shelf (required for 1-bay nodes)	81Y2905
	Filler, node bay	81Y2895
	Lift handle kit (includes 4 chassis lift handles)	81Y2902
	Logo and label kit	00FG045
	Miscellaneous parts kit	81Y2903
	Plastic label plates (left and right)	81Y2913
	Rail kit	88Y6721
	Support brackets (includes chassis mounting hardware)	81Y2906
	Torx 1/4" drive handle	9900712
	Torx bit set	93F2830

Power cords

The power cords that are available for use with the Flex System Enterprise Chassis are determined by your country or region.

For your safety, provides a power cord with a grounded attachment plug to use with this product. To avoid electrical shock, always use the power cord and plug with a properly grounded outlet.

power cords used in the United States and Canada are listed by Underwriter's Laboratories (UL) and certified by the Canadian Standards Association (CSA).

For units intended to be operated at 220 volts (U.S.): Use a UL-listed and CSA-certified cord set consisting of a minimum 18 AWG, Type SVT or SJT, three-conductor cord, a maximum of 15 feet in length and a tandem blade, grounding-type attachment plug rated 15 amperes 250 volts.

For units intended to be operated at 220 volts (outside the U.S.): Use a cord set with a grounding-type attachment plug. The cord set should have the appropriate safety approvals for the country in which the equipment will be installed.

ac power cords for a specific country or region are usually available only in that country or region. The dc power cords are available for all countries and regions.

The following tables list the PDU jumper and power cord CRU part numbers.

Table 11. PDU ac jumper cords

The PDU ac jumper cords table is a two-column table that lists the ac jumper cords that are available for the Lenovo Flex System Enterprise Chassis Types 7893, 8721, and 8724. Column 1 contains the CRU part number. Column 3 describes the jumper cord.

CRU part number	Description
39M5388	2.0m, 16A/100-250V
39M5389	2.5m, 16A/100-250V

The following table lists the single-phase ac power cord CRU part number.

Table 12. Single-phase ac power cord

The single-phase ac power cord table is a three-column table that lists the single-phase power cord that is available for the Lenovo Flex System Enterprise Chassis Types 7893, 8721, and 8724. Column 1 lists the country where the power cord can be used. Column 2 contains the CRU part number. Column 3 describes the power cord.

Country	CRU part number	Description
United States	39M5279	4.3m, 16A/208V, C19 to NEMA L6-20P (US) Line

The following table lists the three-phase ac power cord CRU part numbers.

Table 13. Three-phase ac power cords

The three-phase ac power cords table is a three-column table that lists the three-phase power cords that are available for the Lenovo Flex System Enterprise Chassis Types 7893, 8721, and 8724. Column 1 lists the

Table 13. Three-phase ac power cords (continued)

countries where the power cord can be used. Column 2 contains the CRU part number. Column 3 describes the power cord.

Country	CRU part number	Description
United States	69Y1612	4.3m, US/CAN, NEMA L15-30P - (3P+Gnd) to 3X IEC 320 C19 Line Cord
Australia/New Zealand	69Y1616	4.3m, A/NZ, (PDL/Clipsal) 32A (3P+N+Gnd) to 3X IEC 320 C19 Line Cord
Europe/Middle East/ Africa	69Y1614	4.3m, EMEA/AP, IEC 309 32A (3P+N+Gnd) to 3X IEC 320 C19 Line Cord
Note: Flex System 3X power cords cannot be used with the following power supply part numbers: • 69Y5822 • 69Y5823 • 69Y5836 • 69Y5837 • 69Y5870		

The following table lists the HVDC power cord CRU part number.

Table 14. HVDC power cord

The HVDC power cord table is a three-column table that lists the high-voltage dc power cord that is available for the Lenovo Flex System Enterprise Chassis Types 7893, 8721, and 8724. Column 1 lists the countries where the power cord can be used. Column 2 contains the CRU part number. Column 3 describes the power cord.

Country	CRU part number	Description
All countries	00Y9100	4.3m, ST 3x14 AWG shielded (24 AWG drain wire), 15A/400 V dc line cord
Note: Use the Flex System HVDC power cord only with HVDC power supply CRU number 94Y8274.		

The following table lists the -48 V dc power cord CRU part number.

Table 15. -48 V dc power cord

The -48 V dc power cord table is a three-column table that lists the -48 V dc power cord that is available for the Lenovo Flex System Enterprise Chassis Types 7893, 8721, and 8724. Column 1 lists the countries where the power cord can be used. Column 2 contains the CRU part number. Column 3 describes the power cord.

Country	CRU part number	Description
All countries	69Y1652	6-foot, 75 V dc, 120 A, two 6 AWG conductors, 5.7 mm pin flexible line cord
Note: Use the Flex System -48 V dc power cord only with -48 V dc power supply CRU number 94Y8265.		

Chapter 6. Removing and replacing components

Use this information to remove and replace components of the Flex System Enterprise Chassis.

Replaceable components consist of consumable parts and field replaceable units (FRUs):

- **Consumable part:** Purchase and replacement of consumable parts (components, such as batteries and printer cartridges, that have depletable life) is your responsibility. If Lenovo acquires or installs a consumable part at your request, you will be charged for the service.
- **Field replaceable unit (FRU):** FRUs must be replaced only by a trained service technician, unless they are classified as customer replaceable units (CRUs).
  - **Tier 1 customer replaceable unit (CRU):** Replacement of Tier 1 CRUs is your responsibility. If Lenovo installs a Tier 1 CRU at your request without a service contract, you will be charged for the installation.
  - **Tier 2 customer replaceable unit:** You may install a Tier 2 CRU yourself or request Lenovo to install it, at no additional charge, under the type of warranty service that is designated for your Flex System Enterprise Chassis.

For information about the terms of the warranty, see the *Warranty Information* document that comes with your system.

Installation guidelines

Before you remove or replace a FRU or install an optional device, read the following information:

- Before you begin, read "Safety" on page iii and "Handling static-sensitive devices" on page 958. This information will help you work safely.
- When you install your new compute node, take the opportunity to download and apply the most recent firmware updates. This step will help to ensure that any known issues are addressed and that your compute node is ready to function at maximum levels of performance. To download the latest firmware and device drivers for your compute node, go to http://datacentersupport.lenovo.com/products/servers/flex/x240-m5-compute-node/ 9532/downloads.
- Observe good housekeeping in the area where you are working. Place removed covers and other parts in a safe place.
- Back up all important data before you make changes to disk drives.
- Before you remove a compute node from the chassis, you must shut down the operating system and turn off the compute node. You do not have to shut down the chassis itself.
- Blue or terra cotta on a component indicates touch points, where you can grip the component to remove it from or install it in the compute node, open or close a latch, and so on.
- For a list of supported optional devices for the compute node, see http://www.lenovo.com/serverproven/.

System reliability guidelines

Use these guidelines to make sure that the compute node meets the cooling and system reliability requirements:

- To ensure proper cooling, do not operate the chassis without a compute node or a filler in each node bay.
- Make sure that the ventilation holes on the compute node are not blocked.
- The compute node CMOS battery must be operational. If the CMOS battery becomes defective, replace it immediately. See the documentation that comes with the compute node for instructions.

Handling static-sensitive devices

To reduce the possibility of damage from electrostatic discharge, observe these precautions.

Attention: Static electricity can damage the compute node and other electronic devices. To avoid damage, keep static-sensitive devices in their static-protective packages until you are ready to install them.

- When you work on a chassis that has an electrostatic discharge (ESD) connector, use a wrist strap, especially when you handle modules, optional devices, or compute nodes. To work correctly, the wrist strap must have a good contact at both ends (touching your skin at one end and firmly connected to the ESD connector on the front or back of the chassis).
- 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 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 chassis or any *unpainted* metal surface on any other grounded rack component in the rack in which you are installing the device 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 directly into the compute node without setting down the device. If it is necessary to set down the device, put it back into its static-protective package. Do not place the device on the compute node cover or on a metal surface.
- Take additional care when you handle devices during cold weather. Heating reduces indoor humidity and increases static electricity.

Returning a device or component

If you are instructed to return a device or component, follow all packaging instructions, and use any packaging materials for shipping that are supplied to you.

Removing and replacing consumable parts

Purchase and replacement of consumable parts (components, such as batteries and printer cartridges, that have depletable life) is your responsibility. If Lenovo acquires or installs a consumable component at your request, you will be charged for the service.

Replacing the filter media

If your Flex System Enterprise Chassis is equipped with the optional airborne contaminant filter assembly, use these instructions to remove and replace the dust filter. You can replace the dust filter while the chassis is powered on.

The airborne contaminant filter is a consumable part. It is not covered under the terms of the warranty. Use Table 16 “Suggested inspection and replacement intervals” on page 958 as a guide to help you determine when to replace the filter media in the filter assembly.

Table 16. Suggested inspection and replacement intervals

Environment	Visually inspect and clean	Replace filter
Low dust, low foot traffic	3 months	6 months
Moderate dust, moderate foot traffic	6 weeks	3 months
Heavy dust, heavy foot traffic	2 weeks	1 month

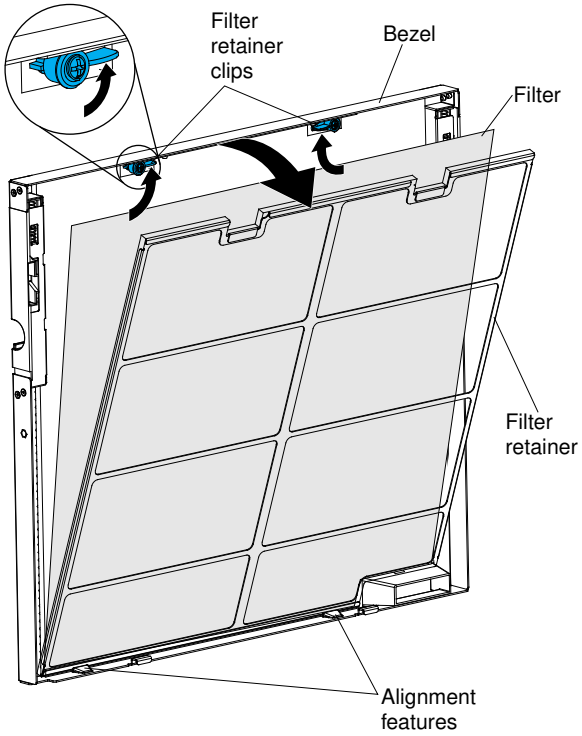
Note: The Chassis Management Module web interface supports an air filter reminder that sends an event message to the CMM event log when the filter media needs to be replaced. See Setting the chassis air filter reminder"Setting the chassis air filter reminder" in the *Lenovo Flex System Chassis Management Module User's Guide* for more information.

Complete the following steps to replace the airborne contaminant filter media in the low-profile or extended-profile configuration:

Step 1. Push down on the slide latches on both sides of the filter assembly.

Step 2. Rotate the filter assembly down and remove the hooks from the slots.

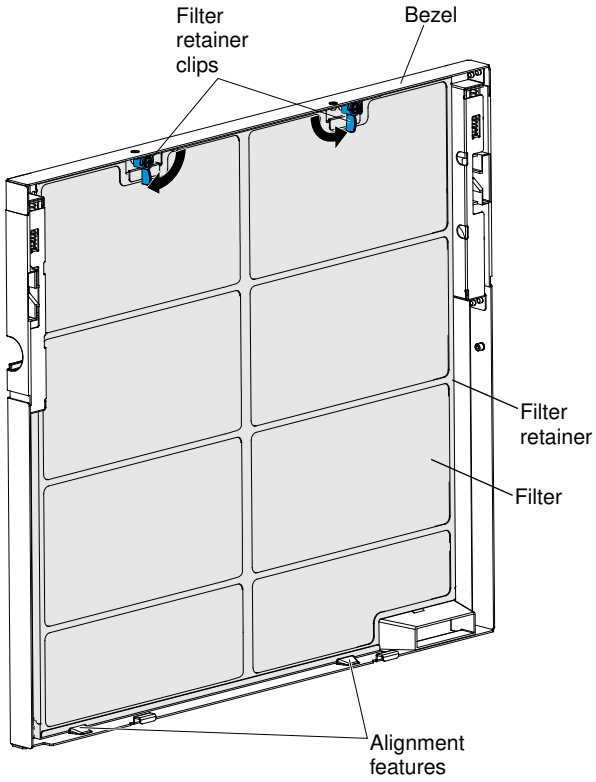
Step 3. Turn the blue filter retainer clips to the open position and remove the filter retainer and filter.



Step 4. Discard the old filter and place a new filter on the filter assembly.

Step 5. Place the bottom of the filter retainer behind the alignment features on the bottom of the filter bezel.

Step 6. Rotate the filter retainer onto the filter and close the blue filter retainer clips by rotating them down to secure the filter retainer to the filter assembly bezel.

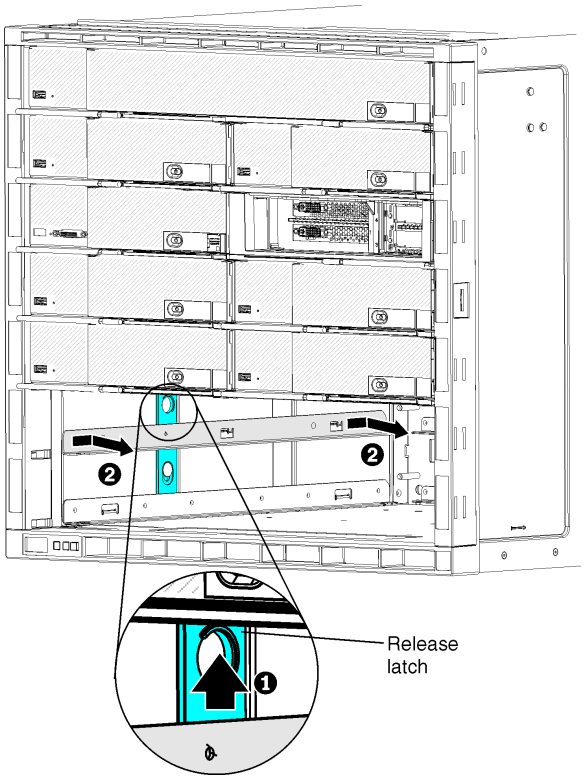


Removing the shelf supports

Use these instructions to remove the shelf supports from the Flex System Enterprise Chassis.

Before you remove the shelf supports, you must remove the chassis shelf and any components that are installed on the shelf. See “Removing a chassis shelf” on page 985 for instructions.

To remove the shelf supports from the chassis, complete the following steps.



Step 1. Starting with the left shelf support, slide the blue latch up to release the support; then, push the shelf support towards the rear of the chassis to disengage the shelf support tabs from the chassis slots.

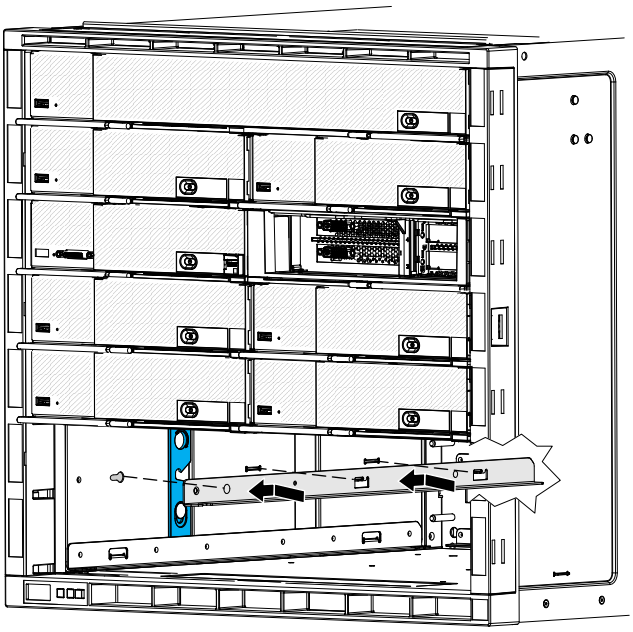
Step 2. Remove the shelf support from the chassis and save it for future use.

Step 3. Repeat steps 1 and 2 for the right shelf support.

Replacing the shelf supports

Use these instructions to install the shelf supports in the Flex System Enterprise Chassis.

To install the shelf supports in the chassis, complete the following steps.



Step 1. Orient the left shelf support to the corresponding slots inside the chassis. The latch post on the shelf support must be towards the front of the chassis.

Step 2. Insert the shelf support tabs into the chassis slots; then, pull the shelf support towards the chassis front until the latch clicks into place.

Step 3. Repeat steps 1 and 2 for the right shelf support.

After you install the shelf supports, complete the following tasks:

- If you are installing 1-bay nodes or fillers in the chassis, see "Replacing a chassis shelf" on page 985.
- If you are installing a 2-bay node in the chassis, see "Installing a 2-bay compute node" on page 43.

Removing and replacing Tier 1 CRUs

Replacement of Tier 1 CRUs is your responsibility. If Lenovo installs a Tier 1 CRU at your request, you will be charged for the installation. However, Lenovo will replace a Tier 2 CRU at your request for no additional charge.

A working Flex System Enterprise Chassis might have numerous power cables, Ethernet cables, and fiber cables that are connected to components on the front and rear of the chassis:

- You might have to disconnect some of the cables when you remove and replace a Tier 1 CRU.
- Make sure that the surrounding cables allow adequate clearance before you remove and replace a Tier 1 CRU.
- Do not pinch, bind, or pull on the cables when you remove and replace a Tier 1 CRU.
- Do not allow unsupported cables to exceed a safe bend radius. For example, a disconnected fiber cable might bend back on itself and become damaged.

Removing a Chassis Management Module

Use these instructions to remove a Flex System Chassis Management Module from the Flex System Enterprise Chassis.

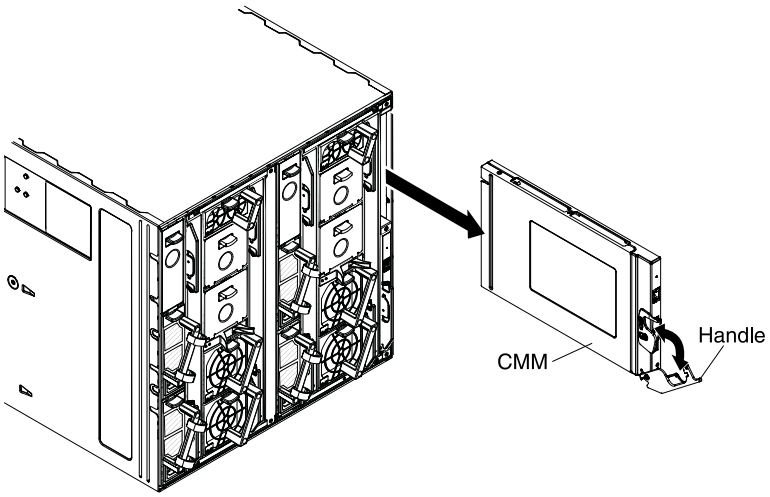
Note: These instructions assume that the chassis is connected to power.

Before you remove a CMM, complete the following steps.

Important: If you have just installed a standby CMM in the chassis, do not remove the primary CMM until the **Active** LED on the standby CMM is lit (indicating that the standby CMM is controlling the chassis). The standby CMM requires about 2 minutes to become active and receive initial status information and firmware from the primary CMM.

1. If the CMM that you are replacing is the only CMM in the chassis and the CMM is functioning, save the configuration file before you proceed.
   - In the CMM web interface, configurations are saved in the Manage Configuration page (select **Configuration** from the **Mgt Module Management** menu). All fields and options are described in the CMM web interface online help.
   - You can also use the `write` command in the CMM command-line interface (CLI). See Lenovo Flex System Chassis Management Module write command"write command" in the *Lenovo Flex System Chassis Management Module Command-Line Interface Reference Guide* for information about commands.
2. If you are removing the primary CMM in the chassis, stop all CMM local and remote sessions before you proceed, to avoid an unexpected termination of sessions.
3. Remove any external devices that block access to the rear of the chassis.
4. Disconnect all cables from the CMM.

To remove the CMM, complete the following steps.



Step 1. Press the release latch down and rotate the handle down until it stops, to disengage the CMM from the chassis.

Step 2. Slide the CMM out of the chassis and place it on a flat, static-protective surface.

Note: If the chassis has only one CMM and you remove the CMM, the fan modules will automatically accelerate to full speed. The fan modules will continue to run at full speed until the CMM is replaced.

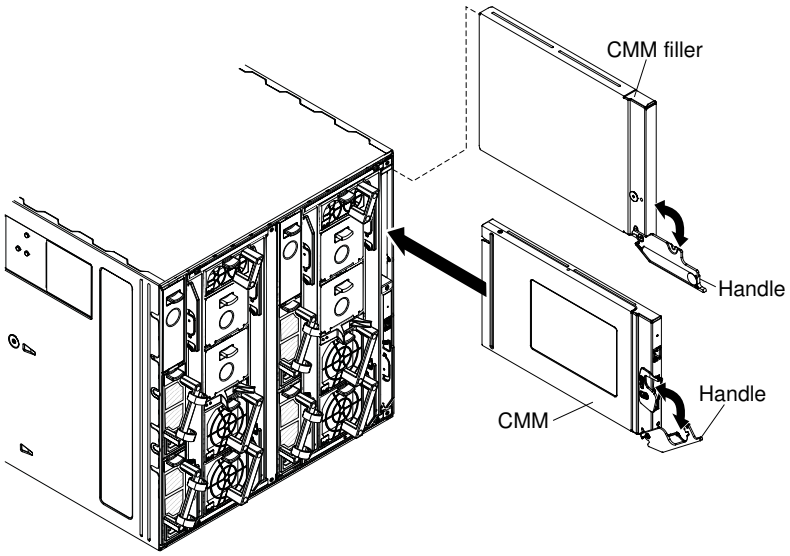
Replacing a Chassis Management Module

Use these instructions to install a CMM in the Flex System Enterprise Chassis. You can install a CMM while the chassis is powered on.

Before you install the CMM, complete the following steps:

1. Read the installation instructions in the documentation that comes with the CMM.
2. If you are installing a standby CMM, see ../com.lenovo.acc.cmm.doc/redundancy_prep_cmm.html"Preparing for CMM redundancy," in the *Lenovo Flex System Chassis Management Module Installation Guide*.
3. If you have not already done so, touch the static-protective package that contains the replacement CMM to an *unpainted* metal part of the chassis or any *unpainted* surface on any other grounded rack component for at least 2 seconds.
4. Remove the CMM from its static-protective package.

To install a Chassis Management Module (CMM), complete the following steps.



Step 1. If a filler is installed in the CMM bay, remove it. Rotate the release handle on the filler down and slide it out of the bay.

Step 2. Press the CMM release latch down and rotate the CMM handle down until it stops.

Step 3. Align the CMM with the bay and slide it into the bay until it is seated.

Step 4. Close the handle (rotate the handle up) so that it locks in place.

Note: Make sure that the power-on LED on the CMM is lit. This indicates that the CMM is operating correctly. See “CMM controls and indicators” on page 17 to locate the LED.

When you install a CMM, if the chassis is not connected to a DHCP server on the network, it takes up to 3 minutes for the CMM to use the default (static) IP address.

After failover, you might have to wait as long as 5 minutes to establish a network connection to the CMM. Some networks include switches, routers, and hubs that do not allow (or relay) an address resolution protocol (ARP) from the new CMM to update the network cached ARP table. Without this information relay, the new MAC address/IP association will not recognize the CMM. 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 CMM.

After you install the CMM, complete the following steps:

1. Replace any components that you removed to gain access to the CMM bay.
2. Connect all cables to the CMM.
3. Depending on your system configuration, you might have to manually configure the CMM:

- If this is a standby CMM and you followed the instructions in Preparing for CMM redundancy"Preparing for CMM redundancy," in the *Lenovo Flex System Chassis Management Module Installation Guide*, no configuration is necessary.

  Note: The standby CMM receives the configuration and status information automatically from the primary CMM. The transfer of information to the standby CMM can take up to 45 minutes after it is installed.
- If this is the only CMM in the chassis, configure the new CMM:
  - If you saved the CMM configuration file before you replaced the CMM, you can apply the saved configuration file to the replacement CMM.
    - In the CMM web interface, saved configurations are applied in the Manage Configuration page (select **Configuration** from the **Mgt Module Management** menu). All fields and options are described in the CMM web interface online help.
    - In the CMM command-line interface (CLI), use the `read` command (see Lenovo Flex System Chassis Management Module read command"read command" in the *Lenovo Flex System Chassis Management Module Command-Line Interface Reference Guide* for information about commands).
  - If you did not save the CMM configuration file before you replaced the CMM, see Configuring the CMM"Configuring the CMM," in the *Lenovo Flex System Chassis Management Module Installation Guide*, for information.

Removing a Flex System Manager management node

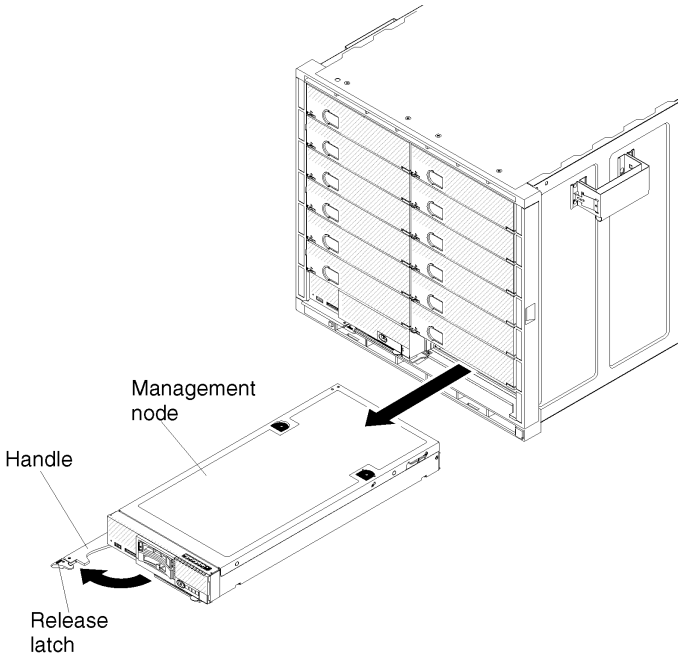
Use these instructions to remove a Flex System Manager management node from the Flex System Enterprise Chassis.

Note: These instructions assume that the chassis is powered on.

Before you remove an Flex System Manager management node, complete the following steps:

1. If the management node that is currently installed in the chassis is functioning, back up the management node image before you replace the management node. See the *Flex System Manager Installation and Service Guide* for instructions.
2. Shut down the management node. See the *Flex System Manager Installation and Service Guide* for instructions.
3. Disconnect all cables from the management node.

To remove the management node, complete the following steps.



Step 1. Open the release handle (rotate the handle to the left) to disengage the management node from the chassis.

Step 2. Slide the management node out of the chassis and place it on a flat, static-protective surface.

Note: When you remove the management node, the fan modules will begin to run at full speed.

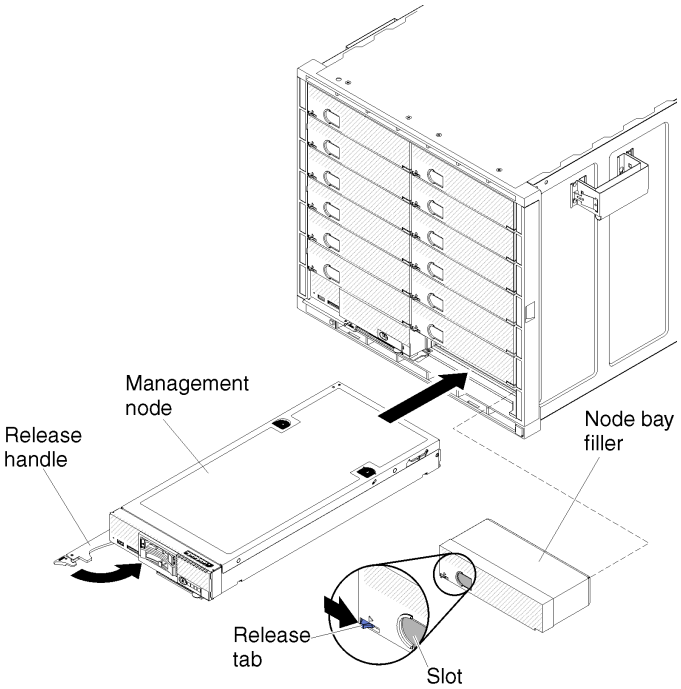
Replacing a Flex System Manager management node

Use these instructions to install a Flex System Manager management node in the Flex System Enterprise Chassis. You can install a management node while the chassis is powered on.

1. Make sure that enough power supplies and fan modules are installed in the chassis to support the management node. See "Installing components" on page 41 to determine the number of power supplies and 80 mm fan modules that are required and where they should be installed in your chassis configuration.
2. Read the documentation that comes with the management node. Flex System Manager documentation is available from http://flexsystem.lenovofiles.com/help/index.jsp.

Note: This procedure assumes that you are replacing an existing management node in the same node bay. If you are installing a new management node, see "Installing a Flex System Manager management node" on page 46.

To install a Flex System Manager management node, complete the following steps.



Step 1. Remove the bay filler, if one is installed. Push the filler release tab to the right; then, grasp the filler by the slot and pull it out of the bay.

Step 2. Open the release handle (rotate the handle to the left).

Step 3. Slide the management node into the chassis bay until it is seated.

Step 4. Close the release handle (rotate the handle to the right).

After you install the Flex System Manager management node, complete the following steps:

1. Connect all cables to the management node.
2. Restart the management node. See the *Flex System Manager Installation and Service Guide* for instructions.
3. Configure the management node by restoring a previously saved image. See the *Flex System Manager Installation and Service Guide* for instructions.

Removing compute nodes

Use the instructions to remove compute nodes from the Flex System Enterprise Chassis, depending on the type of compute node.

Removing a 1-bay compute node

Use these instructions to remove a 1-bay compute node from the Flex System Enterprise Chassis.

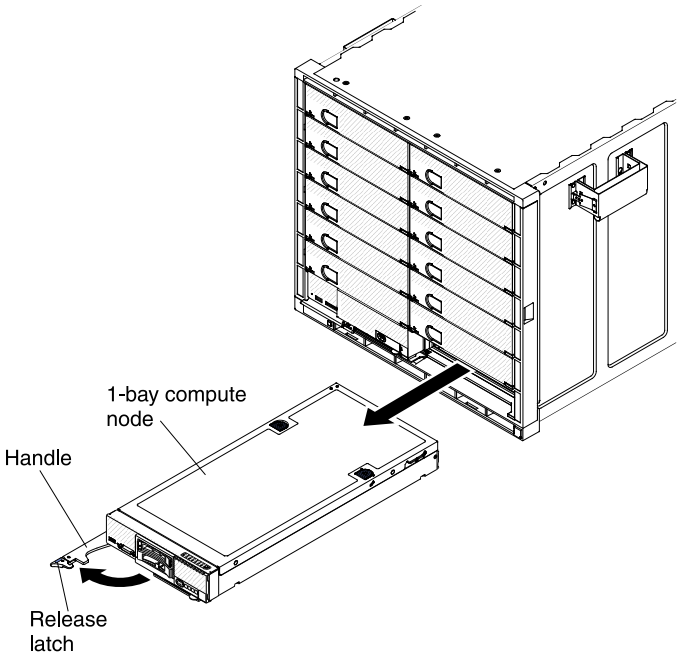
Attention: To maintain proper system cooling, do not operate the chassis without a compute node or compute node filler in each node bay. Install a compute node or filler within one minute of the removal of a compute node.

Before you remove a 1-bay compute node, complete the following tasks:

1. Make a note of the bay number. Reinstalling a compute node into a different bay from the one from which it was removed can have unintended consequences. Some configuration information and update options are established according to bay number.

2. Shut down the compute node operating system; then, shut down the compute node. See the documentation that comes with your compute node for the procedure to shut down the operating system. Compute node documentation is available from http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.common.nav.doc/compute_blades.html.

To remove a 1-bay compute node, complete the following steps.



Step 1. Open the release handles (rotate the handle to the left) to disengage the compute node from the chassis.

Step 2. Slide the compute node out of the compute node bay and place it on a flat, static-protective surface.

Removing a 2-bay compute node

Use these instructions to remove a 2-bay compute node from the Flex System Enterprise Chassis.

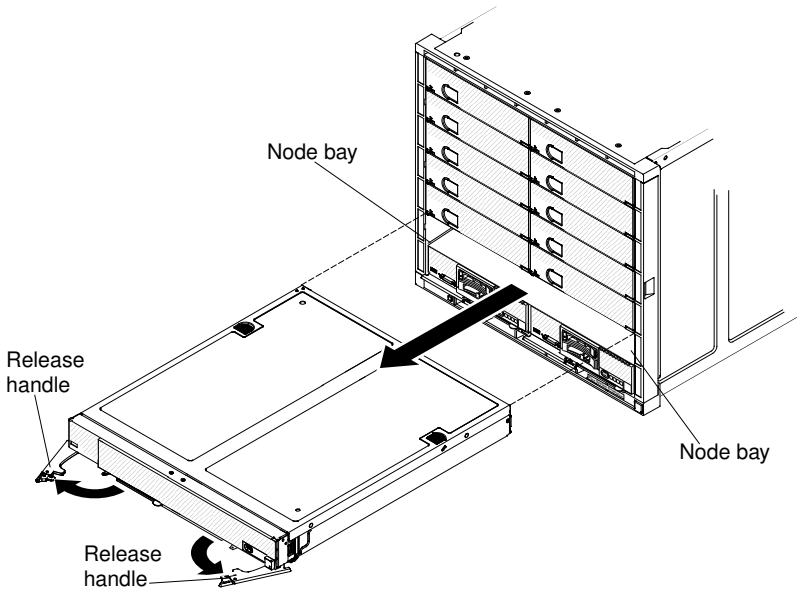
Attention: To maintain proper system cooling, do not operate the chassis without a compute node or compute node filler installed in each node bay. Install a compute node or filler within 1 minute of the removal of a compute node.

Before you remove a 2-bay compute node, complete the following tasks:

1. Make a note of the bay number. Reinstalling a compute node into a different bay from the one from which it was removed can have unintended consequences. Some configuration information and update options are established according to bay number.
2. Shut down the compute node operating system; then, shut down the compute node. See the documentation that comes with your compute node for the procedure to shut down the operating system. Compute node documentation is available from http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.common.nav.doc/compute_blades.html.

To remove a 2-bay compute node, complete the following steps:

Step 1. Open the release handles (rotate the left handle to the left and rotate the right handle to the right) to disengage the compute node from the chassis.



Step 2. Slide the compute node out of the node bay.

Replacing compute nodes

Use the instructions to replace compute nodes in the Flex System Enterprise Chassis, depending on the type of compute node.

Replacing a 1-bay compute node

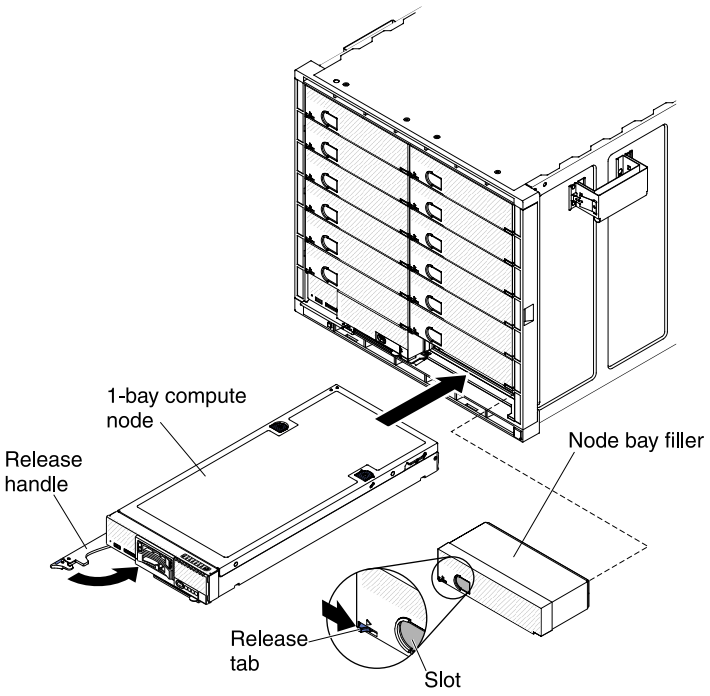
Use these instructions to install a 1-bay compute node in the Flex System Enterprise Chassis. You can install a compute node while the chassis is powered on.

Before you install a 1-bay compute node in the chassis, complete the following steps:

1. Verify that the compute node is compatible with the chassis. See http://www.lenovo.com/serverproven/.
2. Read the instructions that come with the compute node.
3. Make sure that you have installed any optional hardware devices in the compute node.
4. If one or more units of SN550 V2 are to be installed in the chassis, make sure to check if the installed power supply units support SN550 V2. If not, replace them with compatible power supply units.

Note: This procedure assumes that you are replacing an existing compute node in the same node bay. If you are installing a new compute node, see “Installing components” on page 41.

To install a 1-bay compute node, complete the following steps.



Step 1. Remove the node bay filler, if one is installed. Push the filler release tab to the right; then, grasp the filler by the slot and pull it out of the bay.

Step 2. Open the release handle (rotate the handle to the left).

Step 3. Slide the compute node into the node bay until it is seated.

Step 4. Close the release handle (rotate the handle to the right).

After you install the compute node, make a note of the compute node identification information on one of the labels that come with the Flex System Enterprise Chassis. Place a label on the node label tab and on the adjacent chassis label plate, to the right or left of the compute node (depending on the bay in which the compute nodes is installed). See “User labels” on page 59 for more information.

Important: Do not place the label on the compute node or in any way block the ventilation holes.

Replacing a 2-bay compute node

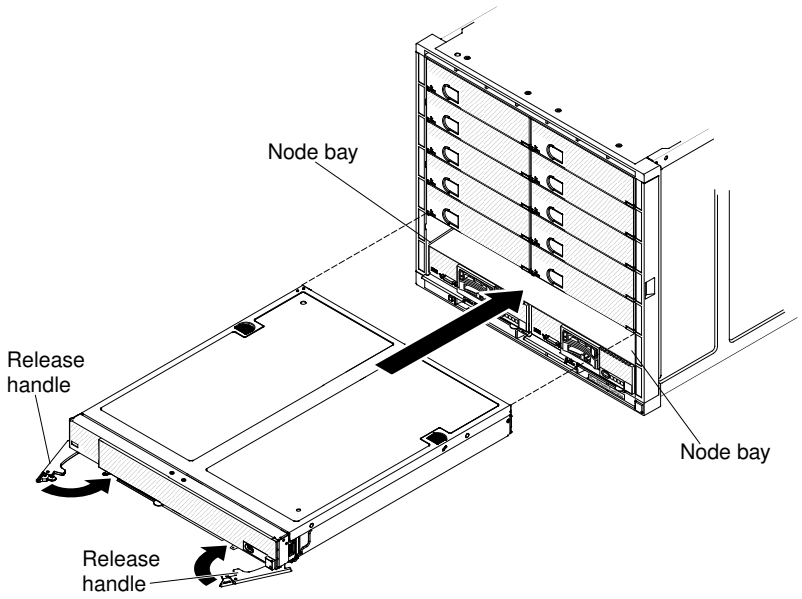
Use these instructions to install a 2-bay compute node in the Flex System Enterprise Chassis. You can install a compute node while the chassis is powered on.

Before you install a compute node into the chassis, complete the following steps:

1. Verify that the compute node is compatible with the chassis. See http://www.lenovo.com/serverproven/.
2. Read the instructions that come with the compute node.
3. Make sure that you have installed any optional hardware devices in the compute node.

Note: This procedure assumes that you are replacing an existing compute node in the same node bays. If you are installing a new compute node, see “Installing components” on page 41.

To install a 2-bay compute node, complete the following steps.



Step 1. Open both release handles (rotate the left handle to the left and rotate the right handle to the right).

Step 2. Slide the compute node into the node bays until it is seated.

Step 3. Close both release handles.

After you install the compute node, make a note of the compute node identification information on the labels that come with the Flex System Enterprise Chassis. Place a label on the node label tab and on the adjacent chassis label plate, to the left of the compute node. See "User labels" on page 59 for more information.

Important: Do not place the label on the compute node or in any way block the ventilation holes on the chassis.

Removing fan modules

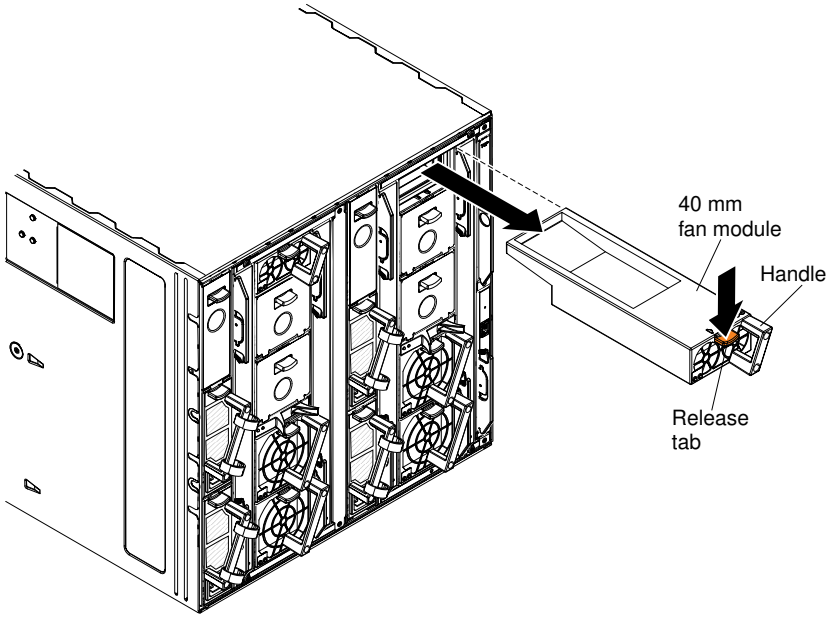
Use the instructions to remove fan modules from the Flex System Enterprise Chassis, depending on the type of fan module.

Removing a 40 mm fan module

Use these instructions to remove a 40 mm fan module from the Flex System Enterprise Chassis.

Attention: Do not operate the chassis for an extended period of time without both 40 mm fan modules installed. If you remove a 40 mm fan module, install a new 40 mm fan module within 1 minute to maintain adequate cooling.

To remove a 40 mm fan, complete the following steps.



Step 1. Grasp the fan module handle and press the release tab.

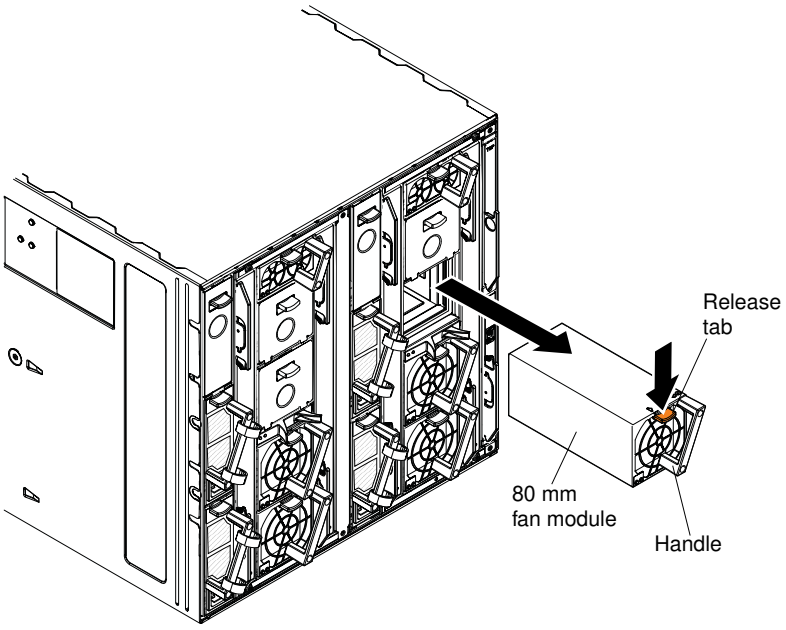
Step 2. Slide the fan module out of the chassis and place it on a flat, static-protective surface.

Note: When you remove a fan module from the chassis, the remaining fan modules will begin to run at full speed, which will be clearly audible.

Removing a 80 mm fan module

Use these instructions to remove a 80 mm fan module from the Flex System Enterprise Chassis.

To remove a 80 mm fan, complete the following steps.



Step 1. Grasp the fan module handle and press the release tab.

Step 2. Slide the fan module out of the chassis and place it on a flat, static-protective surface.

Note: When you remove a fan module from the chassis, the remaining fan modules will begin to run at full speed, which will be clearly audible.

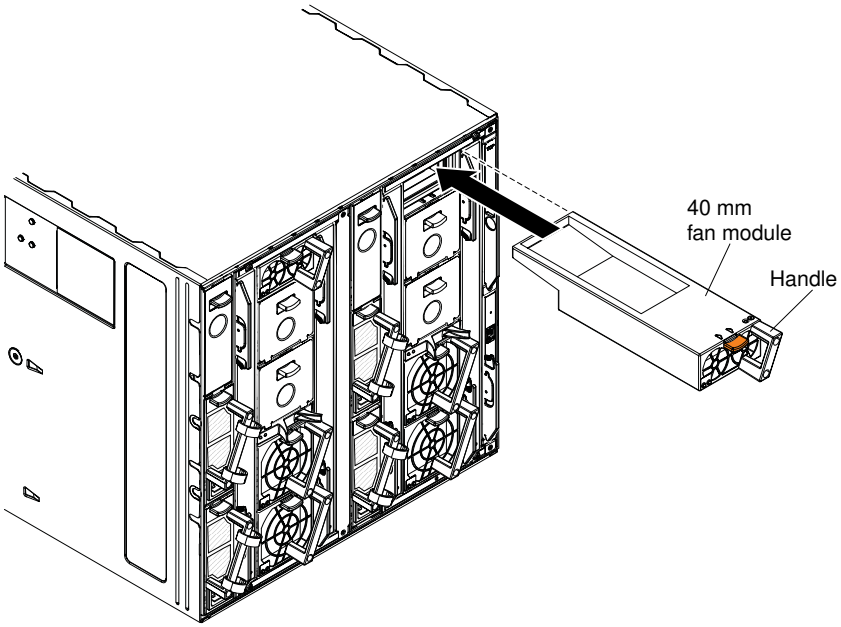
Replacing fan modules

Use the instructions to replace fan modules in the Flex System Enterprise Chassis, depending on the type of fan module.

Replacing a 40 mm fan module

Use these instructions to install a 40 mm fan module in the Flex System Enterprise Chassis. You can install a 40 mm fan module while the chassis is powered on. Both 40 mm fan modules must be installed in the chassis.

To install a 40 mm fan, complete the following steps.



Step 1. Grasp the fan module by the handle and align it with the fan bay.

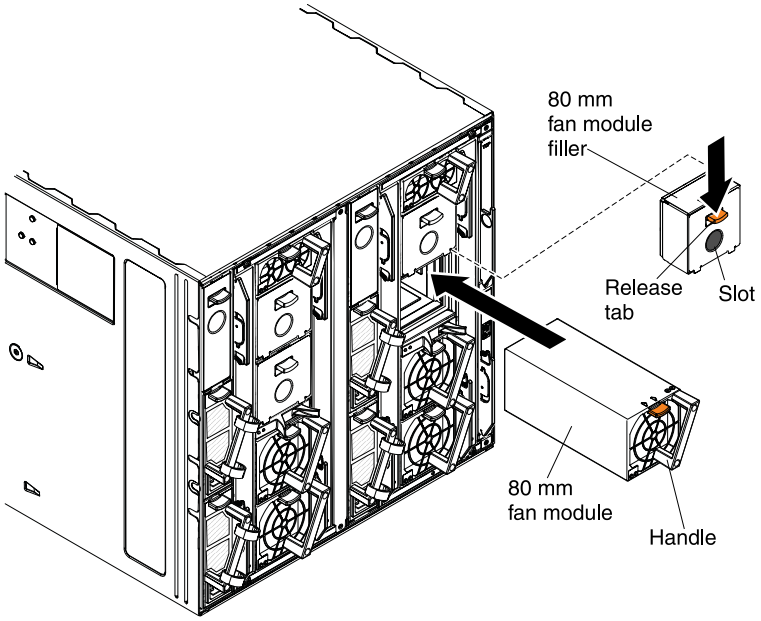
Step 2. Slide the fan module into the chassis until it locks in place.

Replacing a 80 mm fan module

Use these instructions to install a 80 mm fan module in the Flex System Enterprise Chassis. You can install a 80 mm fan module while the Flex System Enterprise Chassis is powered on.

See “Installing components” on page 41 to determine the number of 80 mm fan modules that are required and where they should be installed in your configuration.

To install a 80 mm fan module, complete the following steps.



.

Step 1. Remove the fan module filler, if one is installed.

Step 2. Grasp the fan module by the handle and align it with the fan bay.

Step 3. Slide the fan module into the chassis until it locks in place.

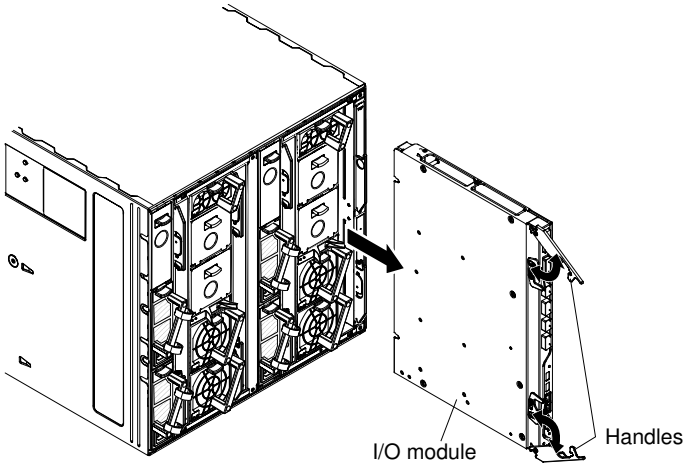
Removing an I/O module

Use these instructions to remove an I/O module from the Flex System Enterprise Chassis.

Before you remove the I/O module, complete the following steps:

1. If possible, power down the I/O module from the Flex System Manager user interface, if one is installed, or from the Chassis Management Module user interface.
2. Disconnect all cables from the I/O module.

To remove an I/O module, complete the following steps.



Step 1. Open the release handles (rotate the top handle up and the bottom handle down) to disengage the I/O module from the chassis.

Step 2. Slide the module out of the I/O bay and place it on a flat, static-protective surface.

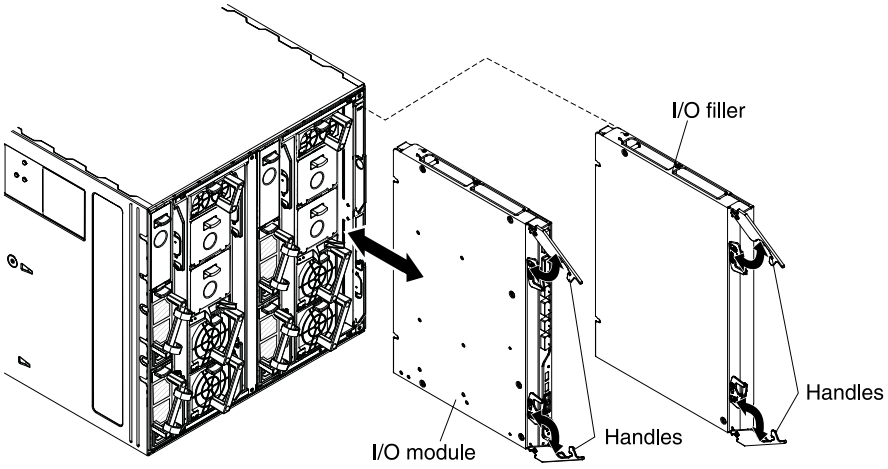
Replacing an I/O module

Use these instructions to install an I/O module in the Flex System Enterprise Chassis. You can install an I/O module while the Flex System Enterprise Chassis is powered on. For redundancy support, you must install I/O modules of the same type in I/O module bays 1 and 2, and I/O modules of the same type in bays 3 and 4 of the chassis.

Before you install an I/O module, complete the following steps:

1. Read the installation instructions that were provided for the I/O module. I/O module documentation is available from http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.networkdevices.doc/network.html.
2. Verify that the I/O module is compatible with the chassis. See http://www.lenovo.com/serverproven/.

To install an I/O module, complete the following steps.



Step 1. Remove the I/O filler, if necessary. Open the release handles (rotate the top handle up and the bottom handle down).

Step 2. Slide the filler out of the bay.

Step 3. Open the release handles on the I/O module (rotate the top handle up and the bottom handle down).

Step 4. Align the I/O module with the bay on the chassis and slide the module into the module bay until it is seated.

Step 5. Close the release handles (rotate the top handle down and bottom handle up).

After you install the I/O module, connect all cables to the module.

Removing a power supply

Use these instructions to remove a power supply from the Flex System Enterprise Chassis.

Statement 31

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 power source.**
- **Connect to properly wired power sources 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 ac power cords, dc power sources, network connections, telecommunications systems, and serial cables before you open the device covers, unless you are instructed otherwise in the installation and configuration procedures.**
- **Connect and disconnect cables as described in the following table when you install, move, or open covers on this product or attached devices.**

To Connect:

1. Turn OFF all power sources and equipment that is to be attached to this product.
2. Attach signal cables to the product.
3. Attach power cords to the product.
   - For ac systems, use appliance inlets.
   - For dc systems, ensure correct polarity of -48 V dc connections: RTN is + and -48 V dc is -. Earth ground should use a two-hole lug for safety.
4. Attach signal cables to other devices.
5. Connect power cords to their sources.
6. Turn ON all the power sources.

To Disconnect:

1. Turn OFF all power sources and equipment that is to be attached to this product.
   - For ac systems, remove all power cords from the chassis power receptacles or interrupt power at the ac power distribution unit.
   - For dc systems, disconnect dc power sources at the breaker panel or by turning off the power source. Then, remove the dc cables.
2. Remove the signal cables from the connectors.
3. Remove all cables from the devices.

Attention: The following circuit breaker and ground cable ratings apply to -48 V dc power supplies only:

Breaker	Listed 70 A	See Note 1
Ground cable	4 AWG with Listed lug which can accept M6 ground screws	See Note 2
Torque rating for ground screws	4.0 - 4.8 Newton-meters (35.4 - 42.5 inch-pounds)	-

1. The maximum steady state current of the -48 V dc power supply is less then 70 A. However during specific events, such as over subscription, it is possible for the power supply to briefly draw a current greater than 70 A. Therefore it is recommended that the power supply be protected by a Listed circuit breaker that will support up to 90 A for a minimum of 20 ms. The suggested Telect High Current Panel Dual 350A Power Distribution Panel (part number 350CB06) using the Telect 70 A circuit breakers (Part number 090-0052-0070) conforms to this specification.
2. If not connecting to a SELV source which provides Reinforced insulation you must use a Ground Cable.

Attention:

- To maintain proper system cooling, do not operate the Flex System Enterprise Chassis without a power supply or power-supply filler in each power supply bay. Install a power supply or filler within 1 minute after

the removal of a power supply. While replacing power supply units, make sure to complete replacement of one unit before starting replacement of another unit.

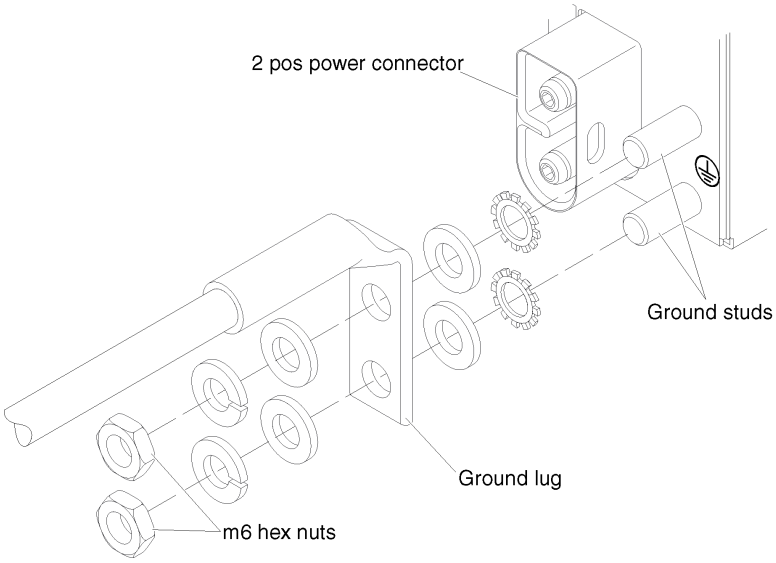
- If you are removing a functioning power supply, make sure that power LEDs on the remaining power supplies are lit and the power management policy that you have chosen supports the removal of the power supply. If the power management policy does not support removal of a power supply, shut down the operating systems and turn off all of the compute nodes before you proceed. (See the documentation that comes with the compute node for instructions for shutting down the compute node operating system and turning off the compute node.)

To remove a power supply, complete the following steps.

Step 1. Disconnect the power cord from the power supply.

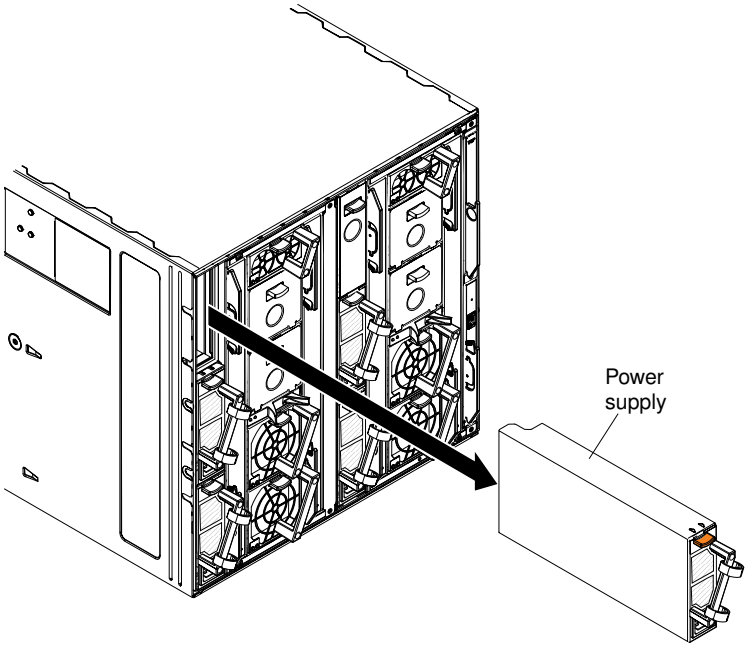
Step 2. If you are removing a -48 to -60 V dc power supply, disconnect the earth ground cable from the power supply.

1. Use a 10 mm nut driver to remove the hex nuts from the ground studs.
2. Remove the lock washer and one flat washer from each ground stud; then, pull the ground lug off the ground studs.
3. Place the washers and hex nuts back on the ground studs for future use.



Step 3. Grasp the handle and press the release tab down.

Step 4. Slide the power supply out of the power-supply bay and place it on a flat, static-protective surface.



If you are instructed to return the power supply, follow all packaging instructions, and use any packaging materials for shipping that are supplied to you.

Replacing a power supply

Use these instructions to install a power supply in the Flex System Enterprise Chassis. You can install a power supply while the Flex System Enterprise Chassis is powered on.

Statement 31

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 power source.**
- **Connect to properly wired power sources 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 ac power cords, dc power sources, network connections, telecommunications systems, and serial cables before you open the device covers, unless you are instructed otherwise in the installation and configuration procedures.**
- **Connect and disconnect cables as described in the following table when you install, move, or open covers on this product or attached devices.**

To Connect:

1. Turn OFF all power sources and equipment that is to be attached to this product.
2. Attach signal cables to the product.
3. Attach power cords to the product.
   - For ac systems, use appliance inlets.
   - For dc systems, ensure correct polarity of -48 V dc connections: RTN is + and -48 V dc is -. Earth ground should use a two-hole lug for safety.
4. Attach signal cables to other devices.
5. Connect power cords to their sources.
6. Turn ON all the power sources.

To Disconnect:

1. Turn OFF all power sources and equipment that is to be attached to this product.
   - For ac systems, remove all power cords from the chassis power receptacles or interrupt power at the ac power distribution unit.
   - For dc systems, disconnect dc power sources at the breaker panel or by turning off the power source. Then, remove the dc cables.
2. Remove the signal cables from the connectors.
3. Remove all cables from the devices.

Statement 34

CAUTION:
To reduce the risk of electric shock or energy hazards:

- **This equipment must be installed by trained service personnel in a restricted-access location, as defined by the NEC and IEC 60950-1, First Edition, The Standard for Safety of Information Technology Equipment.**
- **Connect the equipment to a properly grounded safety extra low voltage (SELV) source. A SELV source is a secondary circuit that is designed so that normal and single fault conditions do not cause the voltages to exceed a safe level (60 V direct current).**
- **Incorporate a readily available approved and rated disconnect device in the field wiring.**
- **See the specifications in the product documentation for the required circuit-breaker rating for branch circuit overcurrent protection.**
- **Use copper wire conductors only. See the specifications in the product documentation for the required wire size.**
- **See the specifications in the product documentation for the required torque values for the wiring-terminal screws.**

Attention: The following circuit breaker and ground cable ratings apply to -48 V dc power supplies only:

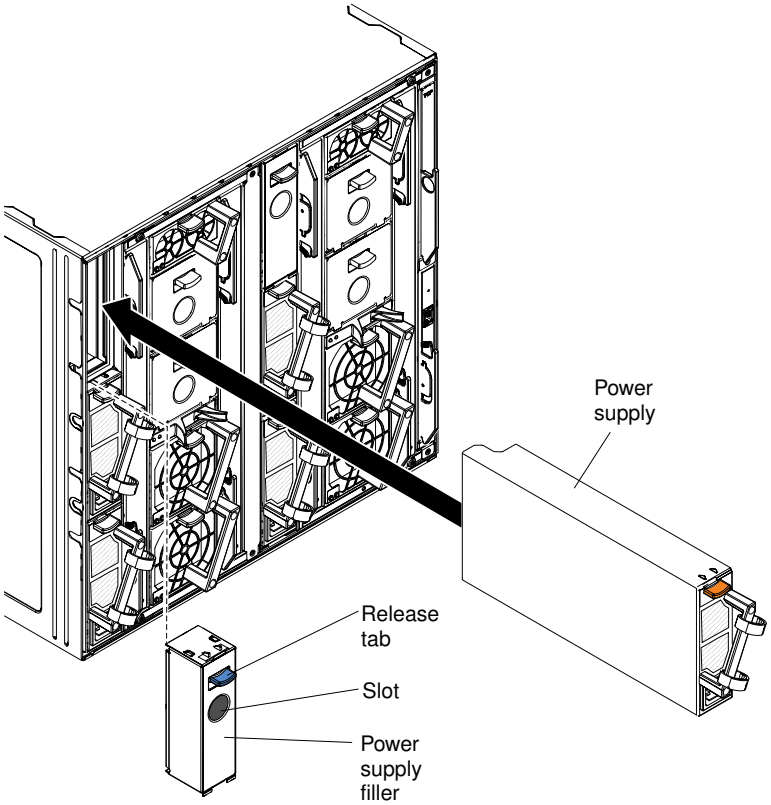
Breaker	Listed 70 A	See Note 1
Ground cable	4 AWG with Listed lug which can accept M6 ground screws	See Note 2
Torque rating for ground screws	4.0 - 4.8 Newton-meters (35.4 - 42.5 inch-pounds)	-

1. The maximum steady state current of the -48 V dc power supply is less then 70 A. However during specific events, such as over subscription, it is possible for the power supply to briefly draw a current greater than 70 A. Therefore it is recommended that the power supply be protected by a Listed circuit breaker that will support up to 90 A for a minimum of 20 ms. The suggested Telect High Current Panel Dual 350A Power Distribution Panel (part number 350CB06) using the Telect 70 A circuit breakers (Part number 090-0052-0070) conforms to this specification.
2. If not connecting to a SELV source which provides Reinforced insulation you must use a Ground Cable.

Important:

- Make sure to complete replacement of one unit before starting replacement of another unit.
- Do not mix different types of power supplies in the Flex System Enterprise Chassis.
- Each chassis must contain either all ac-powered supplies or all dc-powered supplies.
- For ac-powered chassis, do not mix 2100 W and 2500 W power supplies. Chassis powered by ac power should contain only power supplies of the same wattage.
- For dc-powered chassis, do not mix 240 to 380 V dc and -48 to -60 V dc power supplies. Chassis powered by dc power should contain only power supplies of the same input voltage.
- Make sure that the power cord is not connected to the power supply when you install the power supply in the chassis.
- Do not remove the plastic strain-relief ties from the rear of the power supply.

To install a power supply, complete the following steps.



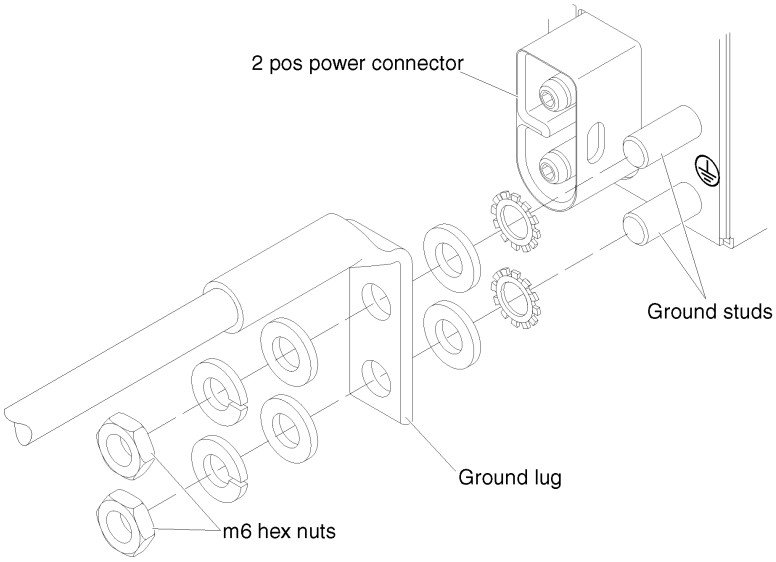
Step 1. If you are adding a power supply, remove the filler from the power-supply bay in which you want to install the power supply (press the release tab, grasp the filler by the slot, and pull it out of the bay).

Step 2. Grasp the power-supply handle and slide the power supply into the bay until it locks in place.

Step 3. If you are installing a -48 to -60 V dc power supply, connect the earth ground cable to the power supply.

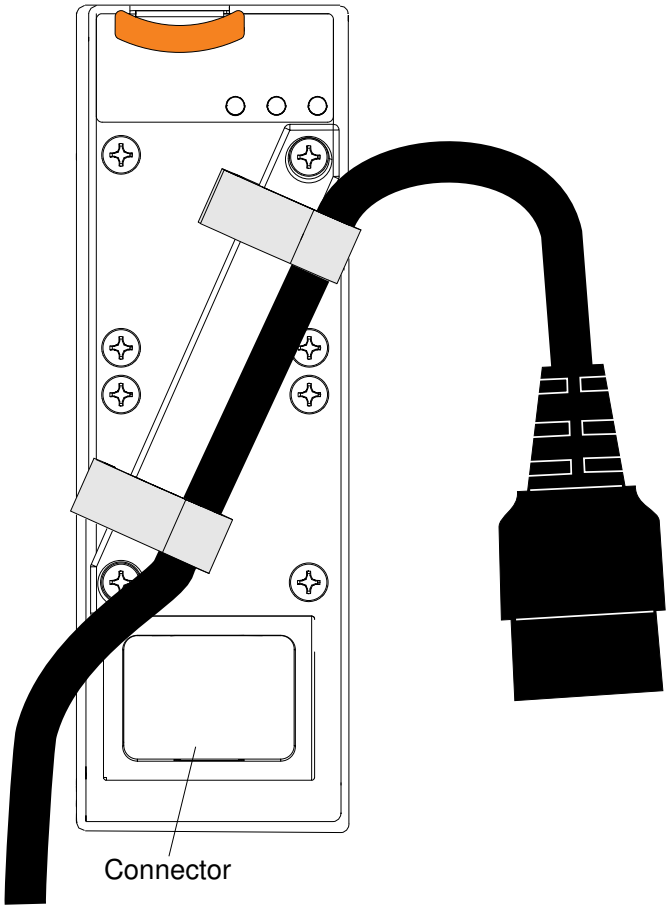
1. Use a 10 mm nut driver to remove the hex nuts from the ground studs.
2. Remove the lock washer and one of the flat washers from each ground stud.
3. Push the ground lug onto the ground studs; then, place the flat washer, the lock washer, and the hex nut back on each ground stud.

4. Use a 10 mm nut driver to tighten the hex nuts to 4.0 - 4.8 Newton-meters (35.4 - 42.5 inch-pounds).

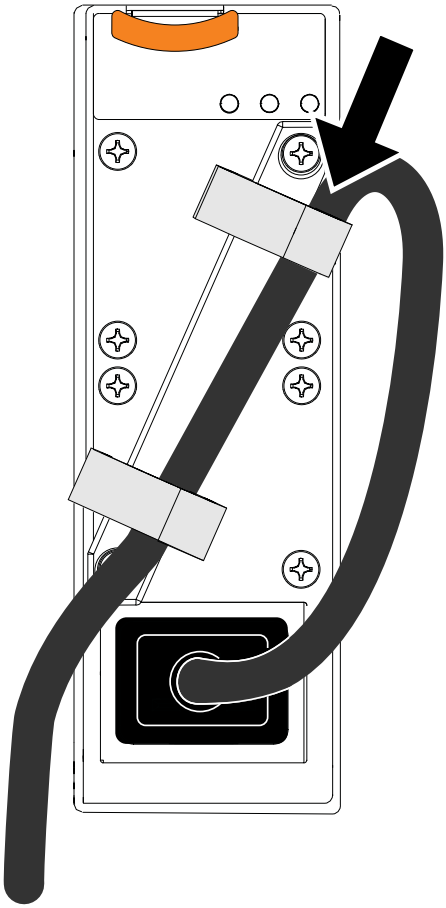


Step 4. Connect the power cord to the power supply:

1. Loosen the strain-relief ties that are attached to the power-supply handle, but do not remove them.
2. Align the power cord with the power-supply handle; then, secure the cord to the handle with the strain-relief ties.



3. Loop the power cord connector around and connect it to the power supply.

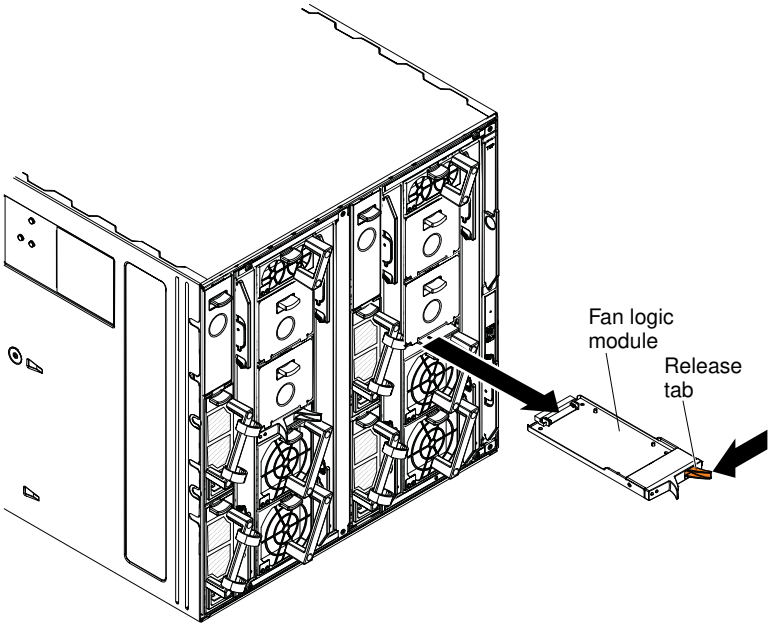


4. Push the power cord back through the strain-relief ties to remove excess cable from the loop.

Removing a fan logic module

Use these instructions to remove a fan logic module from the Flex System Enterprise Chassis. The fan logic module must be replaced as soon as possible.

To remove a fan logic module, complete the following steps.



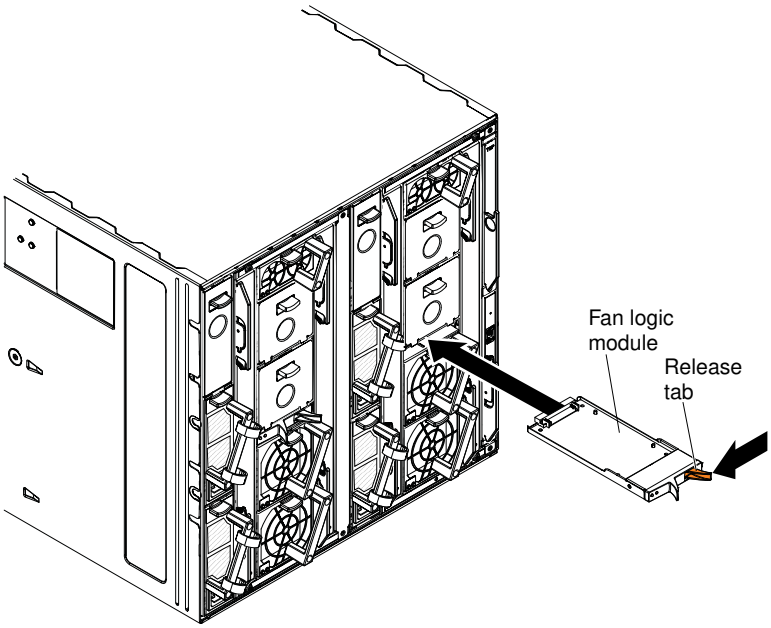
Step 1. Grasp the fan logic module by both tabs.

Step 2. Press the release tab (orange tab) to your left and slide the fan logic module out of the chassis; then, place it on a flat, static-protective surface.

Replacing a fan logic module

Use these instructions to install a fan logic module in the Flex System Enterprise Chassis. Both fan logic modules must be installed in the chassis. Replace any failed fan logic module as soon as possible.

To install a fan logic module, complete the following steps.



Step 1. Grasp the fan logic module by both tabs and align the module with the bay.

Step 2. Press the release tab (orange tab) to your left and slide the fan logic module into the chassis until it locks in place.

Removing a chassis shelf

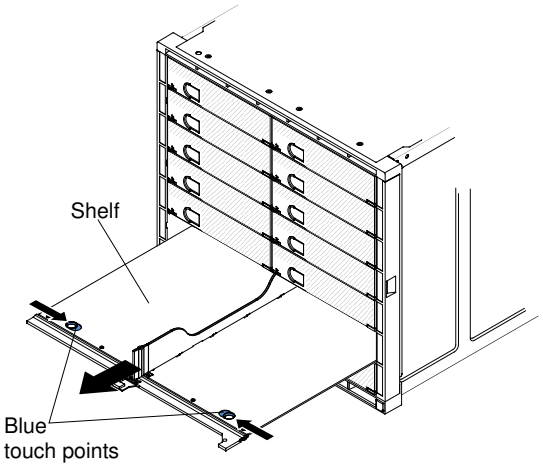
Use these instructions to remove a 1-bay shelf from the Flex System Enterprise Chassis.

Before you remove a chassis shelf, complete the following steps:

1. Read “Safety” on page iii and “Installation guidelines” on page 957
2. Shut down the operating systems and turn off any compute node in the bays in which the shelf is installed. See the documentation that comes with compute node for detailed instructions.
3. Shut down the management node, if one is installed in the bays in which the shelf is installed. See the *Flex System Manager Installation and Service Guide* for instructions.
4. Remove any compute nodes (or fillers) from the bays in which the shelf is installed. Open the compute node handle and slide the compute node out of the chassis.

   Note: Make a note of the bay numbers from which you removed the compute nodes. Reinstalling a compute node into a different bay from the one from which it was removed can have unintended consequences. Some configuration information and update options are established according to bay number.

To remove a shelf from the chassis, complete the following steps.



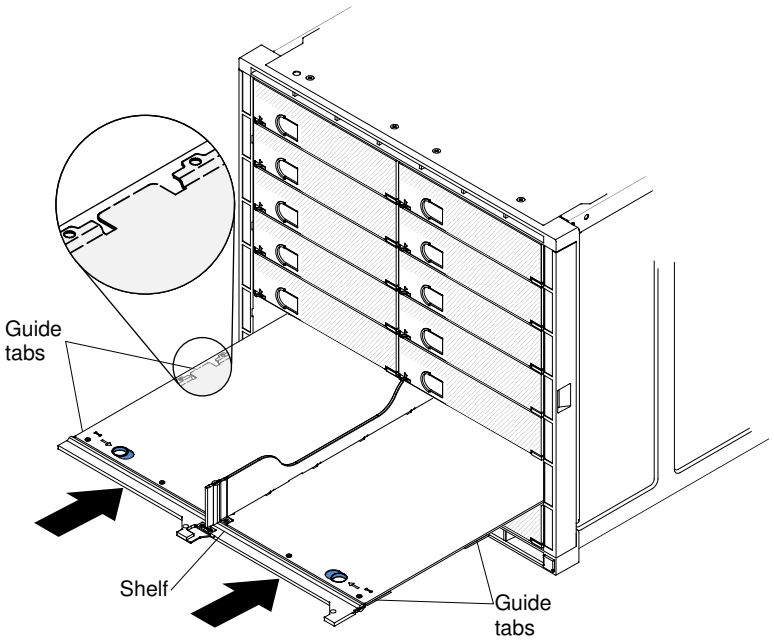
Step 1. Grasp the blue touch points on the shelf and slide both touch points inward toward each other.

Step 2. Slide the shelf out of the chassis and save it for future use.

Replacing a chassis shelf

Use these instructions to install a 1-bay shelf in the Flex System Enterprise Chassis.

To install a shelf into the chassis, complete the following steps.



Step 1. Align the shelf with the shelf supports inside the chassis. Place the shelf on top of the shelf supports and make sure that the shelf guide tabs fit under the shelf supports.

Note: The shelf guide tabs must be under the shelf supports for correct shelf installation.

Step 2. Slide the shelf all the way into the chassis until it snaps in place.

After you install a chassis shelf, complete the following steps:

1. Reinstall the management node, if one was removed, and any compute nodes that you removed from the bays in which the shelf is installed.
2. Turn on any compute nodes that you shut down and restart the operating systems. See the documentation that comes with the compute node for detailed instructions.
3. Restart the management node, if one was removed. See the *Flex System Manager Installation and Service Guide* for instructions.
4. Install node fillers, if you are not installing compute nodes or a management node in the empty node bays.

Removing and replacing FRUs

Field-replaceable units (FRUs) must be removed and replaced only by trained service technicians.

Removing a 4-bay storage enclosure

Use these instructions to remove a 4-bay storage enclosure from the Flex System Enterprise Chassis.

Before you remove a 4-bay storage enclosure, you must prepare the enclosure for removal. See the documentation that comes with your storage enclosure for detailed instructions to shut down and remove the enclosure. Storage node documentation is available from http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.4939.doc/site_product_page.html.

Attention:

- Make sure that you know which type of storage enclosure you are removing. The procedures for removing a storage control enclosure are different from the procedures for removing a storage expansion enclosure.

- If your storage enclosure is powered on and performing I/O operations, follow the detailed instructions that come with the storage enclosure to prepare the enclosure for removal.
- Record which data cables are plugged into the specific ports on the enclosure. The cables must be connected back to the same ports after the replacement is complete; otherwise, the system cannot function properly.
- To maintain proper chassis cooling, do not operate the chassis without a storage enclosure or fillers installed in each node bay. Install a storage enclosure or reinstall the chassis shelves and node fillers within 1 minute of the removal of a storage enclosure.

Step 1. Follow the detailed instructions that come with the 4-bay storage enclosure to shut down the enclosure and remove it from the Flex System Enterprise Chassis.

Replacing a 4-bay storage enclosure

Use these instructions to replace a 4-bay storage enclosure in the Flex System Enterprise Chassis. You can replace a storage enclosure while the chassis is powered on.

Use this procedure to replace a 4-bay storage enclosure with the same type of storage enclosure in the same node bays. If you are installing a new storage enclosure, see “Installing a 4-bay storage enclosure” on page 44 for more information.

Step 1. Follow the detailed instructions that come with the 4-bay storage enclosure to install, cable, and configure the replacement storage enclosure.Storage node documentation is available from http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.4939.doc/site_product_page.html.

After you replace the storage enclosure, complete the following steps:

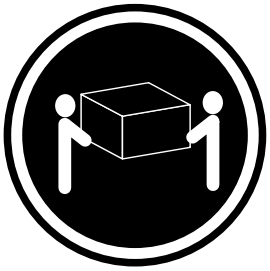
1. Make a note of the storage enclosure identification information on the labels that come with the Flex System Enterprise Chassis. Place a label on the enclosure label tab and on the adjacent chassis label plate, to the left of the storage enclosure. See “User labels” on page 59 for more information.

   Important: Do not place the label on the storage enclosure or in any way block the ventilation holes on the chassis.

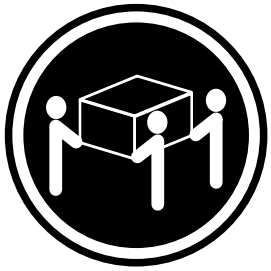
Removing the shuttle

(Trained service technician only) Use these instructions to remove the chassis shuttle from the Flex System Enterprise Chassis.

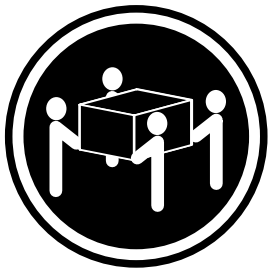
Statement 4



≥ 18 kg (39.7 lb)

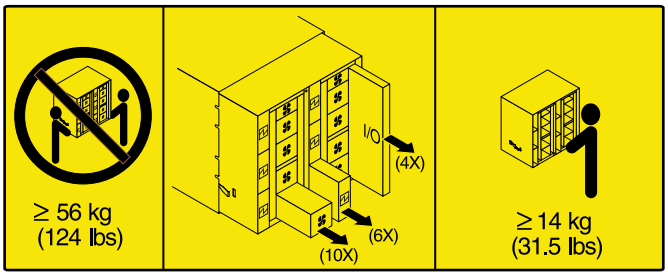


≥ 32 kg (70.5 lb)



≥ 55 kg (121.2 lb)

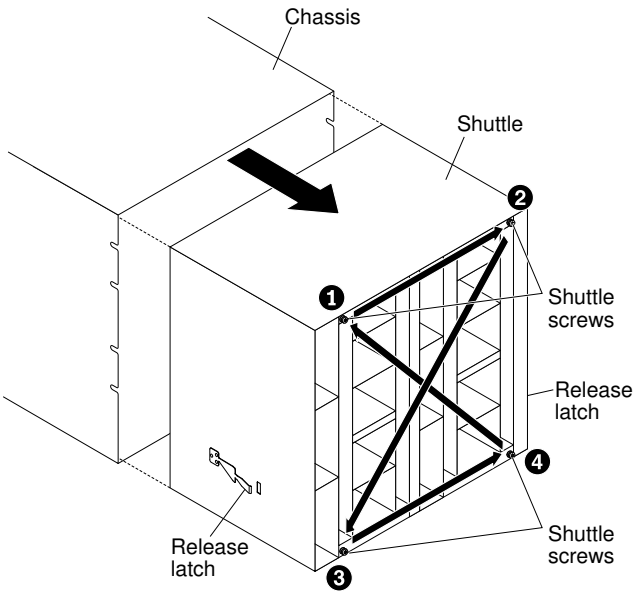
CAUTION:
Use safe practices when lifting.



Before you remove the shuttle, complete the following steps:

1. Read "Safety" on page iii and "Installation guidelines" on page 957
2. Shut down the operating systems and turn off any compute nodes in the chassis. See the documentation that comes with the compute node for detailed instructions.
3. Shut down the management node, if one is installed. See the *Flex System Manager Installation and Service Guide* for instructions.
4. Disconnect the chassis from power (see "Disconnecting the chassis from power" on page 60).
5. Disconnect all cables from the modules in the rear of the chassis.
6. Remove any of the following modules that are installed in the rear of the chassis:
   - I/O modules (see "Removing an I/O module" on page 974).
   - CMM (see "Removing a Chassis Management Module" on page 962).
   - Fan modules (see "Removing a 40 mm fan module" on page 971 and "Removing a 80 mm fan module" on page 972).
   - Power supplies (see "Removing a power supply" on page 975).

To remove the chassis shuttle, complete the following steps.



Step 1. Remove the left, right, and bottom support brackets from the rear of the chassis, if they are installed.

Step 2. Loosen the captive screws on the rear of the shuttle with a T-15 Torx driver:

a. Turn the upper-left screw 3 times.

b. Turn the upper-right screw 3 times.

c. Turn the lower-left screw 3 times.

d. Turn the lower-right screw 3 times.

e. Repeat steps a through d until the screws are loosened (they will not turn anymore).

Step 3. Grasp the shuttle by the holes between fan bays 1 and 2 and between fan bays 6 and 7; then, slide the shuttle out of the chassis until it stops.

Step 4. Place your hands under the shuttle by the safety latches on both sides of the shuttle, then while you support the shuttle, press and hold the safety latches in and slide the shuttle out of the chassis.

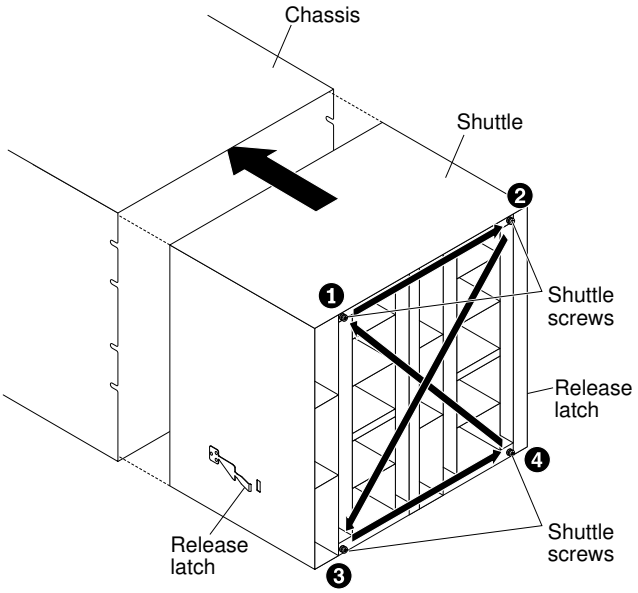
If you are replacing the shuttle with a new shuttle, remove any remaining module fillers for installation in the new shuttle.

Replacing the shuttle

(Trained service technician only) Use these instructions to install the chassis shuttle in the Flex System Enterprise Chassis.

Important: The power supplies, I/O modules, and CMM that are installed in the shuttle connect directly to the midplane. Do not latch these devices in the shuttle before you insert the shuttle; the chassis is not designed for all of those devices to connect to the midplane at the same time.

To install the chassis shuttle, complete the following steps.



Step 1. Align the shuttle with the rear of the chassis and insert the shuttle into the chassis.

Step 2. Push the release latches in; then, slide the shuttle into the chassis until it locks in place.

Step 3. Tighten the captive screws that you removed earlier with a T-15 Torx driver:

a. Turn the upper-left screw 3 times.

b. Turn the upper-right screw 3 times.

c. Turn the lower-left screw 3 times.

d. Turn the lower-right screw 3 times.

e. Repeat the previous steps in turns until the four shuttle screws secure the shuttle tightly against the rear of the midplane.

Step 4. Install the left, right, and bottom support brackets on the rear of the chassis, if you removed them.

After you install the shuttle, complete the following steps:

1. Reinstall the components that you removed from the rear of the Flex System Enterprise Chassis:
   - I/O modules (see “Replacing an I/O module” on page 975).
   - CMM (see “Replacing a Chassis Management Module” on page 963).
   - Fan modules (see “Replacing a 40 mm fan module” on page 973 and “Replacing a 80 mm fan module” on page 973).
   - Power supplies (see “Replacing a power supply” on page 978).
2. Connect any cables that you disconnected from the modules in the rear of the chassis.
3. Connect the chassis to power (see “Connecting the chassis to power” on page 55).
4. Restart any compute nodes that you shut down. See the documentation that comes with each compute node for detailed instructions.
5. Restart the management node, if one is installed. See the *Flex System Manager Installation and Service Guide* for instructions.

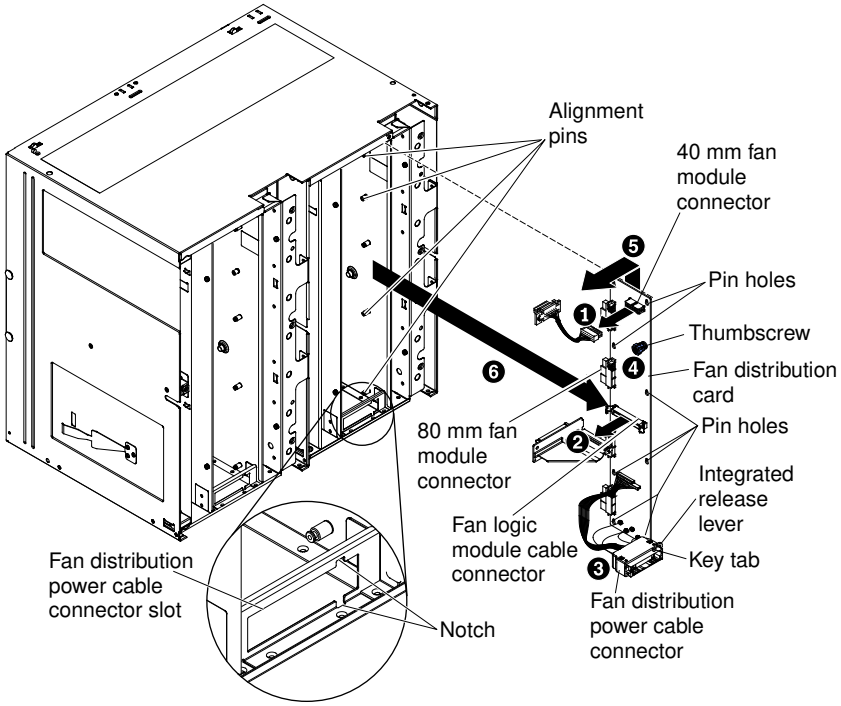
Removing a fan distribution card

(Trained service technician only) Use these instructions to remove a fan distribution card from the Flex System Enterprise Chassis.

Before you remove a fan distribution card, complete the following steps:

1. Read “Safety” on page iii and “Installation guidelines” on page 957
2. Shut down the operating systems and turn off any compute nodes in the chassis. See the documentation that comes with the compute node for detailed instructions.
3. Shut down the management node, if one is installed. See the *Flex System Manager Installation and Service Guide* for instructions.
4. Disconnect the chassis from power (see “Disconnecting the chassis from power” on page 60).
5. Disconnect all cables from the modules in the rear of the chassis.
6. Remove the components from the rear of the chassis.
7. Remove the shuttle from the chassis (see “Removing the shuttle” on page 987).

To remove the fan distribution card, complete the following steps.



Step 1. Disconnect the 40 mm fan module cable from the connector on the fan distribution card. Press the release lever and remove the cable from the connector on the fan distribution card.

Step 2. Disconnect the fan logic module cable from the connector on the fan distribution card:

a. Open the bail latches outward to release the cable.

b. Remove the cable from the connector on the fan distribution card.

Step 3. Remove the fan distribution card power cable connector from the shuttle:

a. Open the cable-management clip and remove the fan distribution power cable from it so that the cable is loose.

b. Press the integrated release lever (on the right side of the power cable connector), using a small tool or your finger.

c. Slide the connector to the right to align the key tab with the notch in the slot for the power cable connector on the shuttle.

d. Push the connector backward through the opening in the shuttle.

Step 4. Loosen the thumbscrew that secures the fan distribution card to the shuttle.

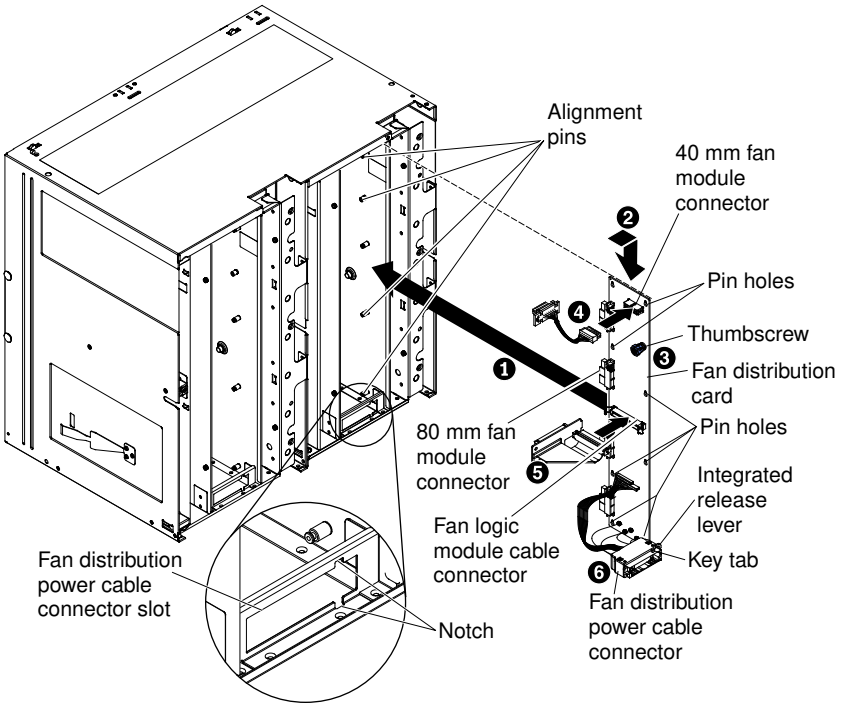
Step 5. Slide the fan distribution card upward and disengage it from the alignment pins on the shuttle.

Step 6. Remove the fan distribution card from the shuttle and place it on a flat, static-protective surface.

Replacing a fan distribution card

(Trained service technician only) Use these instructions to install a fan distribution card in the Flex System Enterprise Chassis.

To install the fan distribution card, complete the following steps.



Step 1. Insert the fan distribution card into the slot on the shuttle.

Step 2. Align the pin holes on the fan distribution card with the alignment pins on the shuttle, align the 80 mm fan module connectors with the openings in the safety mesh on the chassis, and slide the fan distribution card down to lock it in place.

Note: Be sure to hold the card evenly on the top and bottom. When everything is aligned correctly, the fan module connectors will suddenly go through the openings in the mesh, and the alignment pins will go through the pin holes on the fan distribution card.

Step 3. Tighten the thumbscrew that you removed earlier to secure the fan distribution card to the shuttle.

Step 4. Connect the 40 mm fan module cable to the connector on the fan distribution card.

Step 5. Connect the fan logic module cable to the fan distribution card. Make sure that both of the bail latches are in the locked position to secure the cable.

Step 6. Install the fan distribution card power cable connector into the shuttle:

a. Insert the left side of the power cable connector through the slot at the bottom of the shuttle.

b. Push the power connector to the right far enough so that the key tab aligns with the notch in the slot; then, slide the connector to the left until it snaps into place.

c. Route the fan distribution card power cable through the cable-management clip and lock the clip to the secure the cable.

After you install the fan distribution card, complete the following steps:

1. Reinstall the chassis shuttle into the chassis (see “Replacing the shuttle” on page 989).
2. Reinstall the components that you removed from the rear of the chassis.
3. Connect any cables that you disconnected from the modules in the rear of the chassis.
4. Connect the chassis to power (see “Connecting the chassis to power” on page 55).
5. Restart any compute nodes that you shut down. See the documentation that comes with each compute node for detailed instructions.
6. Restart the management node, if one is installed. See the *Flex System Manager Installation and Service Guide* for instructions.

Removing the front LED card

Use these instructions to remove the front LED card from the Flex System Enterprise Chassis. The front LED card must be replaced when it is determined that the card is no longer functioning.

Before you remove the front LED card, complete the following tasks:

1. Shut down the compute node operating system; then, shut down the compute node. See the documentation that comes with your compute nodes for the procedure to shut down the operating system.
2. Shut down the management node, if one is installed. See the *Flex System Manager Installation and Service Guide* for instructions.
3. Disconnect the chassis from power (see “Disconnecting the chassis from power” on page 60).

Note: When you remove the compute nodes, make a note of the bay number for each compute node that you remove. Reinstalling a compute node into a different bay from the one from which it was removed can have unintended consequences. Some configuration information and update options are established according to bay number.

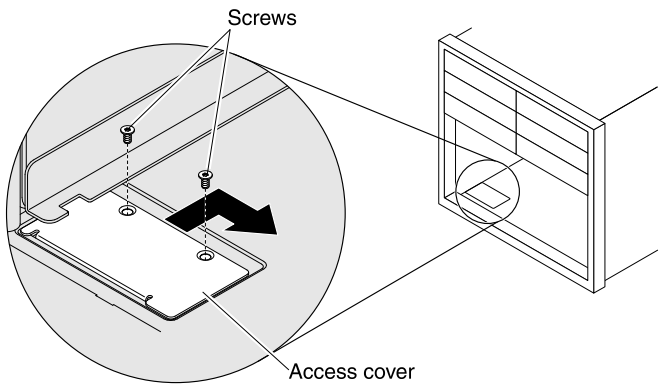
To remove the front LED card, complete the following steps:

Step 1. Remove the compute nodes from node bays 1 through 8 (see “Removing a 1-bay compute node” on page 967 or “Removing a 2-bay compute node” on page 968, depending on the compute node installed).

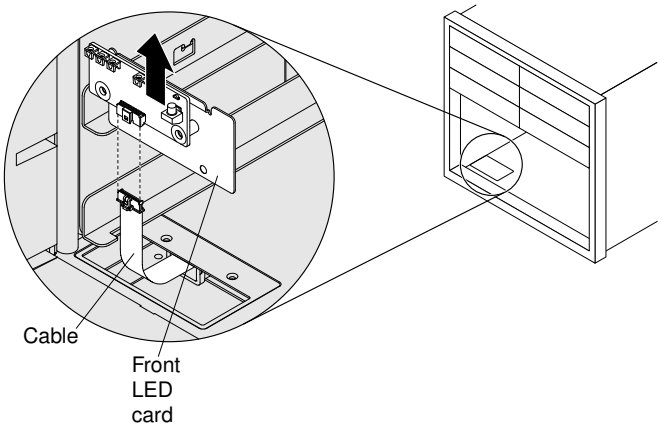
Step 2. Remove the management node, if one is installed in node bays 1 through 8 (see “Removing a Flex System Manager management node” on page 965 for instructions).

Step 3. Remove the four chassis shelves from the bottom of the chassis, if any are installed. For each shelf, grasp the shelf next to the blue touch-point tabs and slide the tabs inward toward each other; then, slide the shelf out of the chassis.

Step 4. Remove the two T-8 Torx screws that secure the card to the chassis, using a Torx driver.



Step 5. Slide the front panel LED card access cover back and to the right and disconnect the cable from the card.



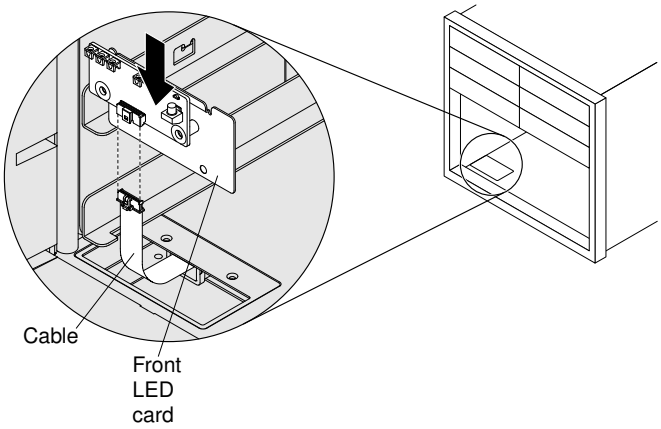
Step 6. Remove the front LED card from the chassis and place it on a flat, static-protective surface.

Replacing the front LED card

Use these instructions to install the front LED card in the Flex System Enterprise Chassis.

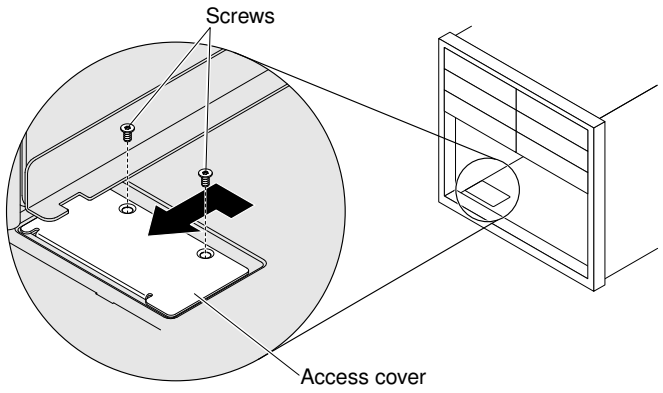
To install the front LED card, complete the following steps:

Step 1. Connect the cable to the front LED card.



Step 2. Align the front LED card with the connector on the chassis and push it into the connector until it is firmly seated.

Step 3. Slide the access cover to the left and then forward to close it.



Step 4. Reinstall the two T-8 Torx screws that you removed earlier.

Step 5. Reinstall the chassis shelves (see “Replacing a chassis shelf” on page 985).

Step 6. Reinstall the compute nodes (see “Replacing a 1-bay compute node” on page 969 or “Replacing a 2-bay compute node” on page 970).

Attention: Be sure to install any compute nodes that you removed in the same bays from which they were removed. Reinstalling a compute node into a different bay from the one from which it was removed can have unintended consequences.

Step 7. Reinstall the management node, if you removed one from node bays 1 through 8 (see “Replacing a Flex System Manager management node” on page 966 for instructions).

After you install the front LED card, complete the following steps:

1. Reconnect power to the chassis.
2. Restart the compute nodes and the operating systems. See the documentation that comes with your compute nodes for detail instructions.
3. Restart the management node, if one is installed. See the *Flex System Manager Installation and Service Guide* for instructions.

Removing the midplane

(Trained service technician only) Use these instructions to remove the midplane from the Flex System Enterprise Chassis.

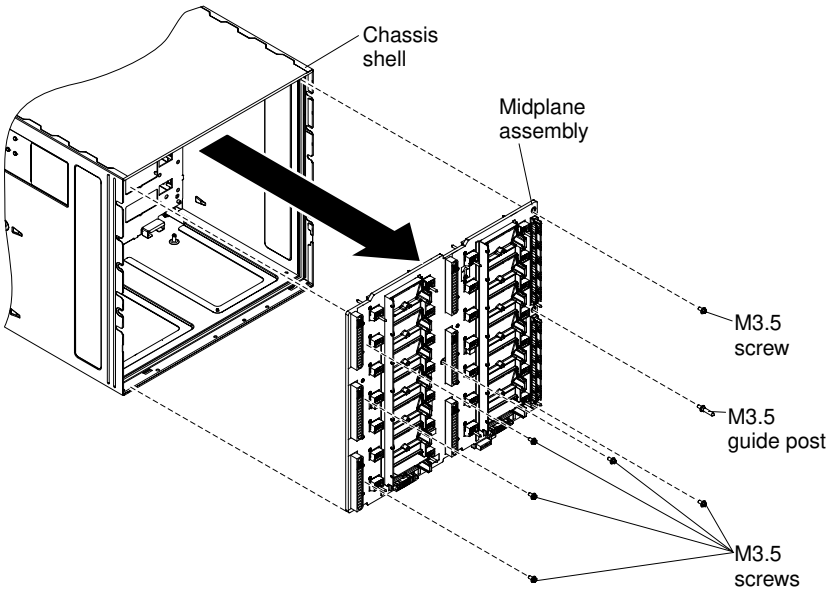
Before you remove the midplane, complete the following steps:

1. Read “Safety” on page iii and “Installation guidelines” on page 957
2. Record the machine type model (8721-HC1 for example), the chassis serial number, and retrieve the existing universally unique identifier (UUID) information from midplane that you are removing. You will need this information to program the new rear LED card that comes with the replacement midplane. The procedure for obtaining this data might require different steps depending on the functional state of the chassis.
   a. Chassis is operating:
      1) Log onto the CMM and access the command-line interface (CLI). You can access the CMM CLI through a direct serial or Ethernet connection to the CMM, through a Telnet connection to the IP address of the CMM, or through a Secure Shell (SSH) connection to the CMM. You must authenticate with the CMM before issuing commands.
      2) Query for the machine type model, chassis serial number, and the UUID values by using the CLI `info` command. Record this information before you proceed.
   b. Chassis is not operating:

1) Obtain the chassis serial number and the machine type model from one of the chassis labels. Use this information to contact Support and request the UUID.
2) Record the chassis serial number, the machine type model, and the UUID before you proceed.

3. Unmanage the chassis in Lenovo XClarity Administrator (see http://flexsystem.lenovofiles.com/help/topic/com.lenovo.lxca.doc/chassis_unmanage.html?cp=1_17). This allows Lenovo XClarity Administrator to use the same UUID for the same chassis when the chassis is remanaged after the midplane is replaced.
4. Shut down the operating systems and turn off any compute nodes in the chassis. See the documentation that comes with the compute node for detailed instructions.
5. Shut down the management node, if one is installed. See the *Flex System Manager Installation and Service Guide* for instructions.
6. Open the release handles on the compute nodes and the management node, if one is installed, to disengage the nodes from the midplane connectors.
7. Disconnect the chassis from power (see "Disconnecting the chassis from power" on page 60).
8. Disconnect all cables from the modules in the rear of the chassis.
9. Remove the components from the rear of the chassis.
10. Remove the shuttle from the chassis (see "Removing the shuttle" on page 987).
11. Remove the rear LED card from the midplane (see "Removing the rear LED card" on page 998).

To remove the midplane, complete the following steps.



.

Step 1. Disengage the compute nodes and Flex System Manager management node in the front of the chassis.

Step 2. Remove the guide post with a 3/16 inch (5 mm) deep socket hex driver.

Step 3. Remove the six screws that secure the midplane to the chassis.

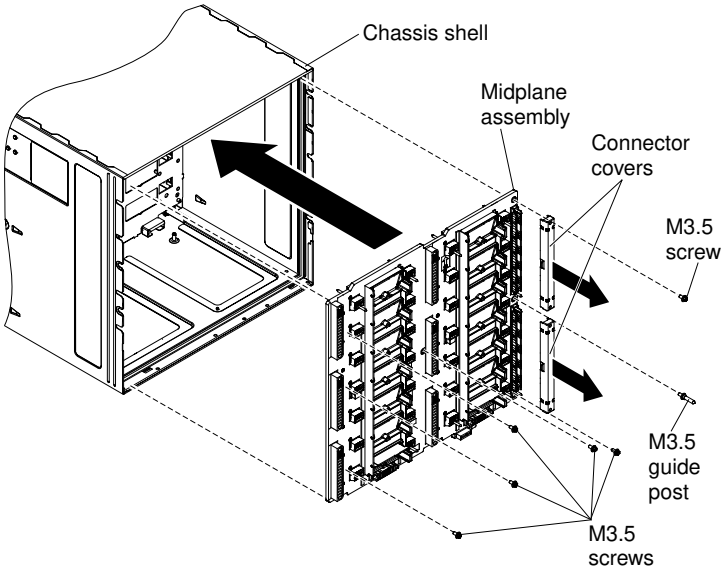
Step 4. Carefully grasp the midplane and slide it away from the chassis and off of the guide pins (keep it straight while you slide it off the guide pins).

Note: Make sure that you do not grasp the connectors on the midplane. You could damage the connectors.

Replacing the midplane

(Trained service technician only) Use these instructions to install the midplane in the Flex System Enterprise Chassis.

To install the midplane, complete the following steps.



Step 1. Remove the connector covers from the midplane, if they are installed.

Step 2. Carefully align the midplane with the guide pins in the chassis and slide the midplane all the way into the chassis until it stops.

Attention:

- You must hold the midplane up against the top inside of the chassis shell and keep the midplane vertical during installation. If the midplane is not inserted correctly, the guide pins can contact the midplane connectors and damage the connector pins.
- Do not grasp the connectors on the midplane when you install it in the chassis. Touching the connectors might damage the connector pins.
- Make sure that the rear LED card cable is out of the way when you slide the midplane into the chassis.

Step 3. Install the six screws that secure the midplane to the chassis.

Step 4. Install the guide post with a 3/16 inch (5 mm) deep socket hex driver.

Important: After you install a new midplane, you must install and program the rear LED card that comes with the new midplane, and program the vital product data (VPD) (see “Replacing the rear LED card” on page 999 for instructions), so that Lenovo XClarity Administrator can use the same UUID for the chassis afterwards.

After the new rear LED card is installed, reassemble the chassis and program the vital product data (VPD) that is stored on the card. Complete the following steps:

1. Reinstall the shuttle into the chassis (see “Replacing the shuttle” on page 989).
2. Reinstall the components that you removed from the rear of the chassis.
3. Connect any cables that you disconnected from the modules in the rear of the chassis.
4. Connect the chassis to power (see “Connecting the chassis to power” on page 55).

5. Remanage the chassis in Lenovo XClarity Administrator (see http://flexsystem.lenovofiles.com/help/topic/com.lenovo.lxca.doc/chassis_manage.html?cp=1_13cp=1_17). This allows Lenovo XClarity Administrator to use the same UUID for the same chassis after the midplane is replaced.
6. Log in to the CMM and access the command-line interface (CLI). You can access the CMM CLI through a direct serial or Ethernet connection to the CMM, through a Telnet connection to the IP address of the CMM, or through a Secure Shell (SSH) connection to the CMM. You must authenticate with the CMM before issuing commands. Use the CLI `vpdrep` command to program the serial number, machine type model, and the universal unique identifier (UUID) into the replacement rear LED card. The CLI command to program this data can be executed in two ways, the data for the three command arguments can be entered individually or together in any combination. At least one command argument must be present. For example, to program all three fields at once: `vpdrep -sn -tm -uuid` where:

vpdrep command arguments	Description
`-sn`	Chassis serial number (7 alphanumeric characters)
`-tm`	Machine type model (7 alphanumeric characters)
`-uuid`	Universally unique identifier (32 hex digits, spaces not allowed)

7. Restart the CMM for the vital product data change to take effect. The vital product data values can be queried by using the CLI `info` command.
8. Close the release handles on the compute nodes, I/O modules, and the management node (if one is installed) in order to seat the nodes and I/O modules in the midplane connectors.
9. Restart any compute nodes that you shut down. See the documentation that comes with the compute node for detailed instructions.
10. Restart the management node, if one is installed. See the *Flex System Manager Installation and Service Guide* for instructions.
11. The I/O Modules are powered-on automatically by the CMM.

Removing the rear LED card

(Trained service technician only) Use these instructions to remove the rear LED card from the chassis midplane.

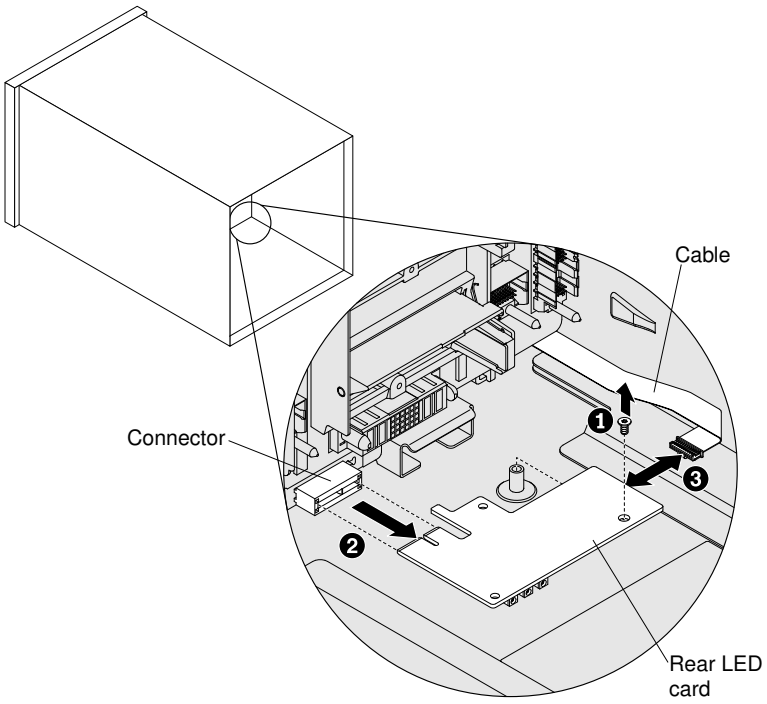
Before you remove the rear LED, complete the following steps:

1. Read “Safety” on page iii and “Installation guidelines” on page 957
2. Record the machine type model (8721-HC1 for example), the chassis serial number, and retrieve the existing universally unique identifier (UUID) information from midplane that you are removing. You will need this information to program the new rear LED card that comes with the replacement midplane. The procedure for obtaining this data might require different steps depending on the functional state of the chassis.
   a. Chassis is operating:
      1) Log onto the CMM and access the command-line interface (CLI). You can access the CMM CLI through a direct serial or Ethernet connection to the CMM, through a Telnet connection to the IP address of the CMM, or through a Secure Shell (SSH) connection to the CMM. You must authenticate with the CMM before issuing commands.
      2) Query for the machine type model, chassis serial number, and the UUID values by using the CLI `info` command. Record this information before you proceed.
   b. Chassis is not operating:
      1) Obtain the chassis serial number and the machine type model from one of the chassis labels. Use this information to contact Support and request the UUID.

2) Record the chassis serial number, the machine type model, and the UUID before you proceed.

3. Unmanage the chassis in Lenovo XClarity Administrator (see http://flexsystem.lenovofiles.com/help/topic/com.lenovo.lxca.doc/chassis_unmanage.html?cp=1_17). This allows Lenovo XClarity Administrator to use the same UUID for the same chassis when the chassis is remanaged after the midplane is replaced.
4. Shut down the operating systems and turn off any compute nodes in the chassis. See the documentation that comes with the compute node for detailed instructions.
5. Shut down the management node, if one is installed. See the *Flex System Manager Installation and Service Guide* for instructions.
6. Open the release handles on the compute nodes and the management node, if one is installed, to disengage the nodes from the midplane connectors.
7. Disconnect the chassis from power (see "Disconnecting the chassis from power" on page 60).
8. Disconnect all cables from the modules in the rear of the chassis.
9. Remove the components from the rear of the chassis.
10. Remove the shuttle from the chassis (see "Removing the shuttle" on page 987).

To remove the rear LED card from the midplane, complete the following steps.



Step 1. Remove the T-10 Torx screw that secures the card with a Torx driver.

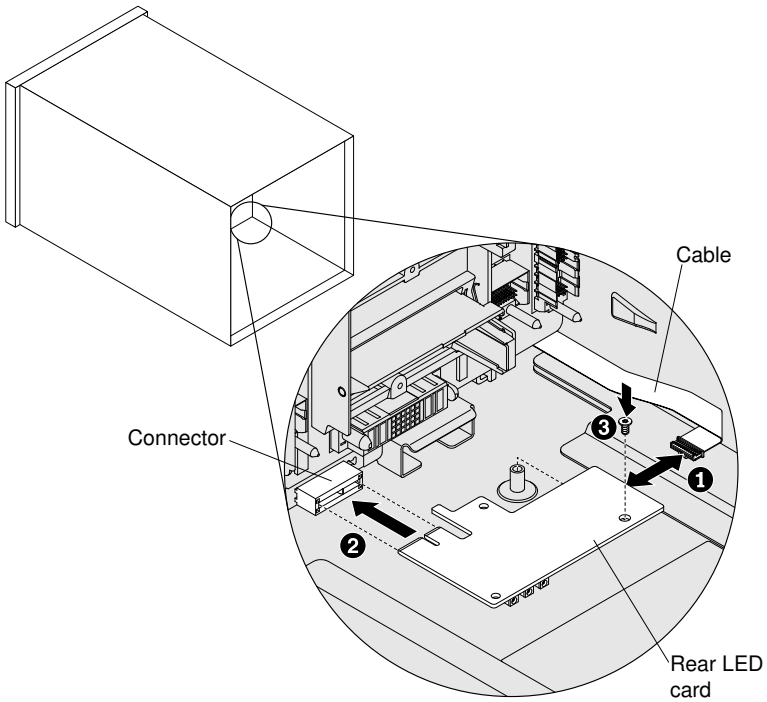
Step 2. Slide the card out toward you, and then disconnect the cable from the card.

Step 3. Remove the card from the midplane and place it on a flat, static-protective surface.

Replacing the rear LED card

(Trained service technician only) Use these instructions to install a replacement rear LED card in the chassis midplane.

To install the rear LED card in the midplane, complete the following steps.



Step 1. Insert the rear LED card into the connector on the midplane.

Step 2. Connect the cable to the rear LED card.

Step 3. Replace the T-10 Torx screw that you removed earlier to secure the rear LED card.

Important: After you install the rear LED card that comes with a new midplane, you must reassemble the chassis and program the vital product data (VPD) that is stored on the card, so that Lenovo XClarity Administrator can use the same UUID for the chassis afterwards.

Complete the following steps:

1. Reinstall the shuttle into the chassis (see "Replacing the shuttle" on page 989).
2. Reinstall the components that you removed from the rear of the chassis.
3. Connect any cables that you disconnected from the modules in the rear of the chassis.
4. Connect the chassis to power (see "Connecting the chassis to power" on page 55).
5. Remanage the chassis in Lenovo XClarity Administrator (see http://flexsystem.lenovofiles.com/help/topic/com.lenovo.lxca.doc/chassis_manage.html?cp=1_13cp=1_17). This allows Lenovo XClarity Administrator to use the same UUID for the same chassis after the midplane is replaced.
6. Log in to the CMM and access the command-line interface (CLI). You can access the CMM CLI through a direct serial or Ethernet connection to the CMM, through a Telnet connection to the IP address of the CMM, or through a Secure Shell (SSH) connection to the CMM. You must authenticate with the CMM before issuing commands. Use the CLI `vpdrep` command to program the serial number, machine type model, and the universal unique identifier (UUID) into the replacement rear LED card. The CLI command to program this data can be executed in two ways, the data for the three command arguments can be entered individually or together in any combination. At least one command argument must be present. For example, to program all three fields at once: `vpdrep -sn -tm -uuid` where:

vpdrep command arguments	Description
`-sn`	Chassis serial number (7 alphanumeric characters)
`-tm`	Machine type model (7 alphanumeric characters)
`-uuid`	Universally unique identifier (32 hex digits, spaces not allowed)

7. Restart the CMM for the vital product data change to take effect. The vital product data values can be queried by using the CLI `info` command.
8. Close the release handles on the compute nodes and the management node, if one is installed, to seat the nodes in the midplane connectors.
9. Restart any compute nodes that you shut down. See the documentation that comes with the compute node for detailed instructions.
10. Restart the management node, if one is installed. See the *Flex System Manager Installation and Service Guide* for instructions.

Appendix A. Getting help and technical assistance

If you need help, service, or technical assistance or just want more information about Lenovo products, you will find a wide variety of sources available from Lenovo to assist you.

Use this information to obtain additional information about Lenovo and Lenovo products, and determine what to do if you experience a problem with your Lenovo system or optional device.

Note: This section includes references to IBM web sites and information about obtaining service. IBM is Lenovo's preferred service provider for the System x, Flex System, and NeXtScale System products.

Before you call

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

If you believe that you require warranty service for your Lenovo product, the service technicians will be able to assist you more efficiently if you prepare before you call.

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system and any optional devices are turned on.
- Check for updated software, firmware, and operating-system device drivers for your Lenovo product. The Lenovo Warranty terms and conditions state that you, the owner of the Lenovo product, are responsible for maintaining and updating all software and firmware for the product (unless it is covered by an additional maintenance contract). Your service technician will request that you upgrade your software and firmware if the problem has a documented solution within a software upgrade.
- If you have installed new hardware or software in your environment, check http://www.lenovo.com/serverproven/ to make sure that the hardware and software is supported by your product.
- Go to http://support.lenovo.com to check for information to help you solve the problem.
- Gather the following information to provide to the service technician. This data will help the service technician quickly provide a solution to your problem and ensure that you receive the level of service for which you might have contracted.
  - Hardware and Software Maintenance agreement contract numbers, if applicable
  - Machine type number (Lenovo 4-digit machine identifier)
  - Model number
  - Serial number
  - Current system UEFI and firmware levels
  - Other pertinent information such as error messages and logs
- Go to https://www-947.ibm.com/support/servicerequest/Home.action to submit an Electronic Service Request. Submitting an Electronic Service Request will start the process of determining a solution to your problem by making the pertinent information available to the service technicians. The IBM service technicians can start working on your solution as soon as you have completed and submitted an Electronic Service Request.

You can solve many problems without outside assistance by following the troubleshooting procedures that Lenovo provides in the online help or in the Lenovo product documentation. The Lenovo product documentation also describes the diagnostic tests that you can perform. The documentation for most systems, operating systems, and programs contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the documentation for the operating system or program.

Using the documentation

Information about your Lenovo system and preinstalled software, if any, or optional device is available in the product documentation. That documentation can include printed documents, online documents, readme files, and help files.

See the troubleshooting information in your system documentation for instructions for using the diagnostic programs. The troubleshooting information or the diagnostic programs might tell you that you need additional or updated device drivers or other software. Lenovo maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. To access these pages, go to http://support.lenovo.com.

Getting help and information from the World Wide Web

Up-to-date information about Lenovo products and support is available on the World Wide Web.

On the World Wide Web, up-to-date information about Lenovo systems, optional devices, services, and support is available at http://support.lenovo.com. The most current version of the product documentation is available in the following product-specific Information Centers:

Flex System products:http://flexsystem.lenovofiles.com/help/index.jsp

System x products:http://systemx.lenovofiles.com/help/index.jsp

NeXtScale System products:http://nextscale.lenovofiles.com/help/index.jsp

How to send DSA data

You can use the Enhanced Customer Data Repository to send diagnostic data to IBM.

Before you send diagnostic data to IBM, read the terms of use at http://www.ibm.com/de/support/ecurep/terms.html.

You can use any of the following methods to send diagnostic data:

- **Standard upload:** http://www.ibm.com/de/support/ecurep/send_http.html
- **Standard upload with the system serial number:** http://www.ecurep.ibm.com/app/upload_hw
- **Secure upload:** http://www.ibm.com/de/support/ecurep/send_http.html#secure
- **Secure upload with the system serial number:** https://www.ecurep.ibm.com/app/upload_hw

Creating a personalized support web page

You can create a personalized support web page by identifying Lenovo products that are of interest to you.

To create a personalized support web page, go to https://support.lenovo.com. From this personalized page, you can subscribe to weekly email notifications about new technical documents, search for information and downloads, and access various administrative services.

Software service and support

Through IBM Support Line, you can get telephone assistance, for a fee, with usage, configuration, and software problems with your Lenovo products.

For more information about Support Line and other IBM services, see http://www.ibm.com/services or see https://datacentersupport.lenovo.com/us/en/supportphonelist for support telephone numbers. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

Hardware service and support

IBM is Lenovo's preferred service provider for the System x, Flex System and NeXtScale System products.

You can receive hardware service through your Lenovo reseller or from IBM. To locate a reseller authorized by Lenovo to provide warranty service, go to https://datacentersupport.lenovo.com/us/en/serviceprovider and click **Business Partner Locator**. For IBM support telephone numbers, see https://datacentersupport.lenovo.com/us/en/supportphonelist. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

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

Taiwan product service

Use this information to contact product service for Taiwan.

委製商/進口商名稱: 荷蘭商聯想股份有限公司台灣分公司
進口商地址: 台北市內湖區堤頂大道2段89號5樓
進口商電話: 0800-000-702 (代表號)

Appendix B. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area.

Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

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

Lenovo (United States), Inc.
1009 Think Place - Building One
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

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

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

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

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

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

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Trademarks

Lenovo, the Lenovo logo, Flex System, System x, NeXtScale System, and x Architecture are trademarks of Lenovo in the United States, other countries, or both.

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

Internet Explorer, Microsoft, and Windows are trademarks of the Microsoft group of companies.

Linux is a registered trademark of Linus Torvalds.

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

Important notes

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

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

When referring to processor storage, real and virtual storage, or channel volume, KB stands for 1 024 bytes, MB stands for 1 048 576 bytes, and GB stands for 1 073 741 824 bytes.

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

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

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

Each solid-state memory cell has an intrinsic, finite number of write cycles that the cell can incur. Therefore, a solid-state device has a maximum number of write cycles that it can be subjected to, expressed as `total bytes written` (TBW). A device that has exceeded this limit might fail to respond to system-generated commands or might be incapable of being written to. Lenovo is not responsible for replacement of a device that has exceeded its maximum guaranteed number of program/erase cycles, as documented in the Official Published Specifications for the device.

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

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

Recycling information

Lenovo encourages owners of information technology (IT) equipment to responsibly recycle their equipment when it is no longer needed. Lenovo offers a variety of programs and services to assist equipment owners in recycling their IT products. For information on recycling Lenovo products, go to: http://www.lenovo.com/recycling.

US & Canada Only

US & Canada Only

Particulate contamination

Attention: Airborne particulates (including metal flakes or particles) and reactive gases acting alone or in combination with other environmental factors such as humidity or temperature might pose a risk to the device that is described in this document.

Risks that are posed by the presence of excessive particulate levels or concentrations of harmful gases include damage that might cause the device to malfunction or cease functioning altogether. This specification sets forth limits for particulates and gases that are intended to avoid such damage. The limits must not be viewed or used as definitive limits, because numerous other factors, such as temperature or moisture content of the air, can influence the impact of particulates or environmental corrosives and gaseous contaminant transfer. In the absence of specific limits that are set forth in this document, you must implement practices that maintain particulate and gas levels that are consistent with the protection of human health and safety. If Lenovo determines that the levels of particulates or gases in your environment have caused damage to the device, Lenovo may condition provision of repair or replacement of devices or parts on implementation of appropriate remedial measures to mitigate such environmental contamination. Implementation of such remedial measures is a customer responsibility.

Table 17. Limits for particulates and gases

Limits for particulates and gases

Contaminant	Limits
Particulate	• The room air must be continuously filtered with 40% atmospheric dust spot efficiency (MERV 9) according to ASHRAE Standard 52.2[1]. • Air that enters a data center must be filtered to 99.97% efficiency or greater, using high-efficiency particulate air (HEPA) filters that meet MIL-STD-282. • The deliquescent relative humidity of the particulate contamination must be more than 60%[2]. • The room must be free of conductive contamination such as zinc whiskers.
Gaseous	• Copper: Class G1 as per ANSI/ISA 71.04-1985[3] • Silver: Corrosion rate of less than 300 Å in 30 days

[1] ASHRAE 52.2-2008 - *Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size*. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

[2] The deliquescent relative humidity of particulate contamination is the relative humidity at which the dust absorbs enough water to become wet and promote ionic conduction.

[3] ANSI/ISA-71.04-1985. *Environmental conditions for process measurement and control systems: Airborne contaminants*. Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.

Telecommunication regulatory statement

This product may not be certified in your country for connection by any means whatsoever to interfaces of public telecommunications networks. Further certification may be required by law prior to making any such connection. Contact a Lenovo representative or reseller for any questions.

Electronic emission notices

When you attach a monitor to the equipment, you must use the designated monitor cable and any interference suppression devices that are supplied with the monitor.

Federal Communications Commission (FCC) statement

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

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

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

Industry Canada Class A emission compliance statement

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

Avis de conformité à la réglementation d'Industrie Canada

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

Australia and New Zealand Class A statement

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

European Union EMC Directive conformance statement

This product is in conformity with the protection requirements of EU Council Directive 2014/30/EU on the approximation of the laws of the Member States relating to electromagnetic compatibility. Lenovo cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the installation of option cards from other manufacturers.

This product has been tested and found to comply with the limits for Class A equipment according to European Standards harmonized in the Directives in compliance. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

Lenovo, Einsteinova 21, 851 01 Bratislava, Slovakia

CE

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

Germany Class A statement

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Deutschsprachiger EU Hinweis:Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2014/30/EU (früher 2004/108/EC) zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der Klasse A der Norm gemäß Richtlinie.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der Lenovo empfohlene Kabel angeschlossen werden. Lenovo übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der Lenovo verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der Lenovo gesteckt/eingebaut werden.

Deutschland:

Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Betriebsmittein Dieses Produkt entspricht dem „Gesetz über die elektromagnetische Verträglichkeit von Betriebsmitteln“ EMVG (früher „Gesetz über die elektromagnetische Verträglichkeit von Geräten“). Dies ist die Umsetzung der EU-Richtlinie 2014/30/EU (früher 2004/108/EC) in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Betriebsmitteln, EMVG vom 20. Juli 2007 (früher Gesetz über die elektromagnetische Verträglichkeit von Geräten), bzw. der EMV EU Richtlinie 2014/30/EU (früher 2004/108/EC), für Geräte der Klasse A.

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen. Verantwortlich für die Konformitätserklärung nach Paragraf 5 des EMVG ist die Lenovo (Deutschland) GmbH, Meitnerstr. 9, D-70563 Stuttgart.

Informationen in Hinsicht EMVG Paragraf 4 Abs. (1) 4:**Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.**

Nach der EN 55022: „Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen und dafür aufzukommen.“

Nach dem EMVG: „Geräte dürfen an Orten, für die sie nicht ausreichend entstört sind, nur mit besonderer Genehmigung des Bundesministers für Post und Telekommunikation oder des Bundesamtes für Post und Telekommunikation betrieben werden. Die Genehmigung wird erteilt, wenn keine elektromagnetischen Störungen zu erwarten sind.“ (Auszug aus dem EMVG, Paragraph 3, Abs. 4). Dieses Genehmigungsverfahren ist nach Paragraph 9 EMVG in Verbindung mit der entsprechenden Kostenverordnung (Amtsblatt 14/93) kostenpflichtig.

Anmerkung: Um die Einhaltung des EMVG sicherzustellen sind die Geräte, wie in den Handbüchern angegeben, zu installieren und zu betreiben.

Japanese electromagnetic compatibility statements

Japan VCCI Class A statement

この装置は、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障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。　　ＶＣＣＩ－Ａ

This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI). If this equipment is used in a domestic environment, radio interference may occur, in which case the user may be required to take corrective actions.

Japanese Electrical Appliance and Material Safety Law statement (for detachable AC power cord)

本製品およびオプションに電源コード・セットが付属する場合は、
それぞれ専用のものになっていますので他の電気機器には使用しないでください。

JEITA harmonics guideline - Japanese Statement for AC power consumption (W)

定格入力電力表示

(社) 電子情報技術参照委員会 家電・汎用品高調波抑制対策ガイドライン実行計画書に基づく定格入力電力値：　　W

お手持ちのユニットの定格入力電力値(W)はユニットの電源装置に貼付されている電源仕様ラベルをご参照下さい

JEITA harmonics guideline - Japanese Statement of Compliance for Products Less than or Equal to 20A per phase

JEITA 高調波電流抑制対策適合品表示 (JEITA harmonics statements– Japan)

定格電流が 20A／相以下の機器 (For products where input current is less than or equal to 20A per phase)

日本の定格電流が 20A/相 以下の機器に対する高調波電流規制高調波電流規格 JIS C 61000-3-2 適合品

JEITA harmonics guideline - Japanese Statement of Compliance for Products More than 20A

定格電流が 20A／相を超える機器 (For products where input current is less than 20A/Phase of one PSU, but total system power is over 20A/Phase)

本製品は、１相当たり20Aを超える機器ですが、個々のユニットが「高調波電流規格 JIS C 61000-3-2適合品」であり、
本製品はその組み合わせであるため、「高調波電流規格 JIS C 61000-3-2適合品」としています

Korea Communications Commission (KCC) statement

이 기기는 업무용(A급)으로 전자파적합기기로
서 판매자 또는 사용자는 이 점을 주의하시기
바라며, 가정외의 지역에서 사용하는 것을 목
적으로 합니다.

This is electromagnetic wave compatibility equipment for business (Type A). Sellers and users need to pay attention to it. This is for any areas other than home.

Russia Electromagnetic Interference (EMI) Class A statement

ВНИМАНИЕ!
Настоящее изделие относится к оборудованию класса А. При использовании в бытовой обстановке это оборудование может нарушать функционирование других технических средств в результате создаваемых индустриальных радиопомех. В этом случае от пользователя может потребоваться принятие адекватных мер.

People's Republic of China Class A electronic emission statement

中华人民共和国“A类”警告声明

声 明

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

Taiwan Class A compliance statement

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

Taiwan BSMI RoHS declaration

單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛Lead (Pb)	汞Mercury (Hg)	鎘Cadmium (Cd)	六價鉻 Hexavalent chromium (Cr^{+6})	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
機架	○	○	○	○	○	○
外部蓋板	○	○	○	○	○	○
機械組合件	–	○	○	○	○	○
空氣傳動設備	–	○	○	○	○	○
冷卻組合件	–	○	○	○	○	○
內存模塊	–	○	○	○	○	○
處理器模塊	–	○	○	○	○	○
電纜組合件	–	○	○	○	○	○
電源	–	○	○	○	○	○
儲備設備	–	○	○	○	○	○
電路卡	–	○	○	○	○	○
光碟機	–	○	○	○	○	○
雷射器	–	○	○	○	○	○

備考1.〝超出0.1 wt %〞及〝超出0.01 wt %〞係指限用物質之百分比含量超出百分比含量基準值。

Note1 : “exceeding 0.1wt%” and “exceeding 0.01 wt%” indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.

備考2.〝○〞係指該項限用物質之百分比含量未超出百分比含量基準值。

Note2 : “○”indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.

備考3.〝-〞係指該項限用物質為排除項目。

Note3 : The “-“ indicates that the restricted substance corresponds to the exemption.

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

X

Part Number: SP47A31778

Printed in China

(1P) P/N: SP47A31778