Lenovo Flex System Carrier-Grade chassis Installation and Service Guide

Machine Type: 7385
Note

**Note:** Before using this information and the product it supports, read the general information in Appendix B “Notices” on page 985; and read the *Safety Information* and the *Systems Environmental Notices and User Guide* on the Lenovo Documentation CD.
Removing the airborne contaminant filter assembly .................. 961
Replacing the airborne contaminant filter assembly .................. 962
Removing the 1U bezel ........................................... 964
Replacing the 1U bezel ........................................... 964
Removing the 1U filter retainer .................................. 965
Replacing the 1U filter retainer .................................. 965
Removing and replacing FRUs ..................................... 966
Removing the shuttle .............................................. 966
Replacing the shuttle .............................................. 968
Removing a fan distribution card ................................. 969
Replacing a fan distribution card ................................. 970
Removing the front LED card .................................... 972
Replacing the front LED card .................................... 973
Removing the midplane ........................................... 974
Replacing the midplane ........................................... 975
Removing the rear LED card ..................................... 977
Replacing the rear LED card ..................................... 978

Appendix A. Getting help and technical assistance ............... 981
Before you call ...................................................... 981
Using the documentation ........................................ 982
Getting help and information from the World Wide Web ..... 982
How to send DSA data ............................................ 982
Creating a personalized support web page ..................... 982
Software service and support .................................... 982
Hardware service and support ................................... 983
Taiwan product service .......................................... 983

Appendix B. Notices .................................................. 985
Trademarks ......................................................... 986
Important notes ..................................................... 986
Recycling information ............................................ 986
Particulate contamination ........................................ 987
Telecommunication regulatory statement ....................... 987
Electronic emission notices ...................................... 988
  Federal Communications Commission (FCC) statement ........ 988
  Industry Canada Class A emission compliance statement .... 988
  Avis de conformité à la réglementation d’Industrie Canada. 988
  Australia and New Zealand Class A statement ................. 988
  European Union EMC Directive conformance statement .... 988
  Germany Class A statement .................................... 989
  Japanese electromagnetic compatibility statements .......... 990
  Korea Communications Commission (KCC) statement ......... 990
  Russia Electromagnetic Interference (EMI) Class A statement 991
  People’s Republic of China Class A electronic emission statement 991
  Taiwan Class A compliance statement .......................... 991
  Taiwan BSMI RoHS declaration ................................ 992

Index ................................................................. 993
Safety

Before installing this product, read the Safety Information.

Antes de instalar este producto, lea las Informaciones de Seguranza.

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 sikkerhedsforskriverne, 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).

לפינ שותקתו מזרז, קרא את הוראות הביטחון.

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 producto, lea las Informaciones sobre Seguridad.

Перед установкой продукта прочтите инструкции по технике безопасности.

Pred inštaláciou tohto zariadenia si pečítajte 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.

Bu ürünü kurmadan önce güvenlik bilgilerini okuyun

Məkbər Məhsulatının Qoruşunun Qorunun belə təqdim etdiyi Təxərrüxlərindən Qovuq Qovuq

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

**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.

**Statement 1**
DANGER

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

To avoid a shock hazard:

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

<table>
<thead>
<tr>
<th>To Connect:</th>
<th>To Disconnect:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Turn everything OFF.</td>
<td>1. Turn everything OFF.</td>
</tr>
<tr>
<td>2. First, attach all cables to devices.</td>
<td>2. First, remove power cords from outlet.</td>
</tr>
<tr>
<td>3. Attach signal cables to connectors.</td>
<td>3. Remove signal cables from connectors.</td>
</tr>
<tr>
<td>4. Attach power cords to outlet.</td>
<td>4. Remove all cables from devices.</td>
</tr>
<tr>
<td>5. Turn device ON.</td>
<td></td>
</tr>
</tbody>
</table>

Statement 2

CAUTION:

When replacing the lithium battery, use only Part Number 33F8354 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.

Statement 3

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.

⚠️ 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.

Class 1 Laser Product
Laser Klasse 1
Laser Klass 1
Luokan 1 Laserlaita
Appareil À Laser de Classe 1

Statement 4

⚠️ CAUTION: Use safe practices when lifting.

≥ 18 kg (39.7 lb)  ≥ 32 kg (70.5 lb)  ≥ 55 kg (121.2 lb)

Statement 8

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

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

Statement 13

⚠️ 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.

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 21

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

Statement 26

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

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 32

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

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.

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.

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.

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 Carrier-Grade chassis Type 7385 is an 11U NEBS level 3 certified server platform suitable for central offices and rugged environments. It is a compact, high-density, high-performance, rack-mounted, scalable server platform system with integrated chassis management. The 11U Flex System Carrier-Grade chassis is suitable for installation in Network Telecommunication Facilities.

The Flex System Carrier-Grade 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 compute nodes share common resources, such as power, cooling, management, and I/O resources in the chassis.

Notes:

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

The Flex System Carrier-Grade 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 six -48 V to -60 V dc power supplies. 200-240 V ac power supplies are also 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)
• 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 Carrier-Grade 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 up to seven 2-bay compute nodes in the chassis. The 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, 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**

  The Lenovo XClarity Administrator, if available, is a virtual appliance that you can use to manage multiple Flex System Carrier-Grade chassis in a secure environment. The Lenovo XClarity Administrator provides a central interface to perform the following functions for all managed endpoints:

  - User management
The Lenovo XClarity Administrator 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.

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 Carrier-Grade chassis to operate.

<table>
<thead>
<tr>
<th>Component</th>
<th>Bay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two power supplies</td>
<td>Power-supply bays 1 and 4</td>
</tr>
<tr>
<td>Two 40 mm fan modules</td>
<td>Fan bays 5 and 10</td>
</tr>
<tr>
<td>Four 80 mm fan modules</td>
<td>Fan bays 1, 2, 6, and 7</td>
</tr>
<tr>
<td>Two fan logic modules</td>
<td>Fan logic bays 1 and 2</td>
</tr>
<tr>
<td>One Chassis Management Module</td>
<td>CMM bay 1</td>
</tr>
<tr>
<td>One I/O module</td>
<td>I/O bay 1</td>
</tr>
<tr>
<td>One compute node</td>
<td>Node bays 1 - 14</td>
</tr>
</tbody>
</table>

Record information about the Flex System Carrier-Grade chassis in Table 2 “Chassis reference information” on page 3. You will need this information for future reference.

<table>
<thead>
<tr>
<th>Chassis reference information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Product name</td>
<td>Flex System Carrier-Grade chassis</td>
</tr>
<tr>
<td>Machine type</td>
<td>Type 7385</td>
</tr>
<tr>
<td>Model number</td>
<td></td>
</tr>
<tr>
<td>Serial number</td>
<td></td>
</tr>
</tbody>
</table>

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 Carrier-Grade 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](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**

- **FC5022 User Guide**
The Lenovo Documentation CD

The documentation CD contains documentation for your Lenovo Flex System Carrier-Grade chassis Type 7385 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:

• Microsoft Windows or Red Hat Linux
• 100 MHz microprocessor
• 32 MB RAM
• Adobe Acrobat 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 Adobe Acrobat 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 Carrier-Grade 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 features and specifications of the chassis.

See Table 3 “Chassis features and specifications” on page 8. Rate of heat-dissipation calculations for forced-air fan cooling are provided in Table 4 “Rate of heat-dissipation calculations for forced-air fan cooling” on page 10.
### Table 3. Chassis features and specifications

<table>
<thead>
<tr>
<th>Features and specifications</th>
<th>Cooling:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Node bays (on front):</strong>  The chassis has fourteen node bays that support any of the following configurations:</td>
<td>Supports up to 10 variable-speed, hot-swap fan modules:</td>
</tr>
<tr>
<td>• Fourteen 1-bay compute nodes</td>
<td>• Two 40 mm fan modules</td>
</tr>
<tr>
<td>• Seven 2-bay compute nodes (with the shelves removed from the chassis)</td>
<td>• Up to eight 80 mm fan modules</td>
</tr>
<tr>
<td>The chassis can also support a combination of 1-bay and 2-bay compute nodes.</td>
<td><strong>Management modules:</strong></td>
</tr>
<tr>
<td><strong>Notes:</strong></td>
<td>• Two hot-swap Chassis Management Modules</td>
</tr>
<tr>
<td>• A 1-bay compute node occupies one node bay in the chassis.</td>
<td><strong>I/O modules:</strong></td>
</tr>
<tr>
<td>• 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.</td>
<td>Supports up to four scalable switch modules with each providing a 4-lane physical interconnect.</td>
</tr>
<tr>
<td><strong>Module bays (on rear):</strong></td>
<td><strong>Size (11U):</strong></td>
</tr>
<tr>
<td>• Two hot-swap Chassis Management Module bays</td>
<td>• Height: 483 mm (19.02 in.)</td>
</tr>
<tr>
<td>• Six hot-swap power-supply bays</td>
<td>• Depth: 854 mm (33.62 in.)</td>
</tr>
<tr>
<td>• Ten hot-swap fan bays</td>
<td>• Width: 447 mm (17.6 in.)</td>
</tr>
<tr>
<td>• Four hot-swap I/O bays</td>
<td>• Weight:</td>
</tr>
<tr>
<td>• Two hot-swap fan logic bays</td>
<td>− Fully configured (stand-alone): approximately 229.16 kg (505.2 lb) $^6$</td>
</tr>
<tr>
<td></td>
<td>− Fully configured (in the rack): approximately 234.28 kg (516.5 lb) $^6$</td>
</tr>
<tr>
<td></td>
<td>− Empty chassis with shelves: approximately 70.44 kg (155.3 lb)</td>
</tr>
<tr>
<td></td>
<td>− Empty chassis without shelves: approximately 48.94 kg (107.9 lb)</td>
</tr>
<tr>
<td><strong>Upgradeable microcode:</strong></td>
<td><strong>Approximate heat output:</strong></td>
</tr>
<tr>
<td>Microcode is upgradeable when fixes or features are added.</td>
<td>• Minimum configuration: 1365 Btu per hour (400 watts)</td>
</tr>
<tr>
<td>• Chassis Management Module firmware</td>
<td>• Maximum configuration: 44,017 Btu per hour (12,900 watts)</td>
</tr>
<tr>
<td>• I/O module firmware</td>
<td><strong>Declared sound power level:</strong></td>
</tr>
<tr>
<td>• Compute node firmware</td>
<td>• 7.5 bels</td>
</tr>
<tr>
<td><strong>Chassis airflow:</strong> Full chassis configuration with all nodes, I/O modules, power supplies, and fan modules installed.</td>
<td>• Minimum - 270 CFM</td>
</tr>
<tr>
<td>• Minimum - 270 CFM</td>
<td>• Maximum - 1,020 CFM</td>
</tr>
</tbody>
</table>
Table 3. Chassis features and specifications (continued)

<table>
<thead>
<tr>
<th>Features and specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security features:</strong></td>
</tr>
<tr>
<td>• Login password for remote connection</td>
</tr>
<tr>
<td>• Secure Sockets Layer (SSL) security for remote management access</td>
</tr>
<tr>
<td>• Lightweight Directory Access Protocol (LDAP)</td>
</tr>
<tr>
<td>• Trusted and signed firmware</td>
</tr>
<tr>
<td><strong>Predictive Failure Analysis (PFA) alerts:</strong></td>
</tr>
<tr>
<td>• Power supplies</td>
</tr>
<tr>
<td>• Node dependent features</td>
</tr>
<tr>
<td><strong>Electrical input with dc supplies:</strong></td>
</tr>
<tr>
<td>• Rated voltage -48 to -60 V dc</td>
</tr>
<tr>
<td>• Maximum steady state current not more than 70 A</td>
</tr>
<tr>
<td>• Requires a UL listed circuit breaker that can supply up to 90 A for a minimum of 20 ms</td>
</tr>
<tr>
<td><strong>Electrical input with ac supplies:</strong></td>
</tr>
<tr>
<td>• Rated voltage and frequency 200 - 240 V ac single phase at 47-63 Hz</td>
</tr>
<tr>
<td>• Inrush current (chassis maximum) 40 A</td>
</tr>
<tr>
<td>• Leakage current (chassis maximum) 580 uA</td>
</tr>
<tr>
<td>• Branch circuit breaker 20 A maximum</td>
</tr>
<tr>
<td><strong>Power supplies:</strong></td>
</tr>
<tr>
<td>• Minimum: Two hot-swap power supplies</td>
</tr>
<tr>
<td>• Maximum: Six hot-swap power supplies</td>
</tr>
<tr>
<td>• 2500 Watt, -48 to -60 V dc power supplies with 2 position power connector (NEBS level 3)</td>
</tr>
<tr>
<td>• Optional 2500 Watt, 200 - 240 V ac power supplies with IEC 60320 type C20 line cord connector (ASHRAE Class A3)</td>
</tr>
</tbody>
</table>

| Environment: |
| Flex System Carrier-Grade chassis equipped with -48 V dc power supplies are NEBS level 3 certified. |
| **Operating, low altitude:** |
| • Relative humidity 5% - 85% ¹ |
| • Temperature 5°C to 45°C (41°F – 113°F) ² |
| • Maximum altitude 1829 m (6k ft) |
| • Maximum rate of temperature change 30°C/hr (80° F/hr ) ³ |
| **Operating, high altitude (includes fan failure):** |
| • Relative humidity 5% - 85% ¹ |
| • Temperature 5°C to 45°C (41°F – 113°F) ² |
| • Altitude range 1829-3960 m (6k-13k ft) |
| • Maximum rate of temperature change 30°C/hr (80° F/hr ) ³ |
| **Operating, short-term excursions (room HVAC failure):** |
| • Relative humidity 5% - 93% ¹ |
| • Temperature -5°C to 55°C (41°F - 131°F) ² |
| • Maximum altitude 1829 m (6k ft) |
| **Non-operating, storage:** |
| • Relative humidity 5% - 80% ¹ |
| • Temperature 1°C to 70°C (33.8°F - 158°F) |
| • Altitude 3050 m (10,006 ft) |
| **Non-operating, shipment:** |
| • Relative humidity 5% - 100% ¹ |
| • Temperature -40°C to 70°C (-40°F - 158°F) |
| • Altitude 10,700 m (35,105 ft) |

1. Water to air ratio must never exceed 0.026 kg H₂O/ kg dry air.
2. Derate maximum allowable temperature 1°C/213 m above 1829 m. Also note that this maximum temperature is for a self-standing system, not located in a rack. If in a rack, deduct 5°C.
3. 30°C/hr for data centers employing disk drives, tape drives are not used.
4. The equipment acclimation period is 1 hour per 30°C of temperature change from the shipping/storage environment to the operating environment.
5. One excursion is defined at no more than four days (96 hrs), all excursions per year should not exceed 15 days (360 hrs).
6. The fully configured chassis weight is based on all nodes and I/O modules being at their maximum design limit.
Table 4. Rate of heat-dissipation calculations for forced-air fan cooling

<table>
<thead>
<tr>
<th></th>
<th>System International (SI Units)</th>
<th>US Customary Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>D_{equip} 800.1 mm (0.800 m)</td>
<td>31.5 inches (2.63 ft.)</td>
</tr>
<tr>
<td>B</td>
<td>D_{main-aisle} 1066.8 mm (1.067 m)</td>
<td>42.0 inches (3.5 ft.)</td>
</tr>
<tr>
<td>C</td>
<td>D_{wire-aisle} 762.0 mm (0.762 m)</td>
<td>30 inches (2.5 ft.)</td>
</tr>
<tr>
<td>D</td>
<td>W_{frame} 482.5 mm (0.483 m)</td>
<td>19.0 inches (1.583 ft.)</td>
</tr>
<tr>
<td>E</td>
<td>P_{in} -47.5Vdc x 86.2A = 4094.5W</td>
<td>-47.5Vdc x 86.2A = 4094.5W</td>
</tr>
<tr>
<td>F</td>
<td>P_{out} -</td>
<td>-</td>
</tr>
<tr>
<td>G</td>
<td>A_{equip} [(A + (B/2) + (C/2))] x D</td>
<td>0.827 m² 8.91 ft.²</td>
</tr>
<tr>
<td>H</td>
<td>H_{R_{equip}} (E – F) 4094.5W</td>
<td>(E – F) 4094.5W</td>
</tr>
<tr>
<td>I</td>
<td>H_{shelf} 482.0 mm (0.482 m)</td>
<td>19.5 inches (1.583 ft.)</td>
</tr>
<tr>
<td>J</td>
<td>H_{D_{per shelf}} (H/G)</td>
<td>(H/G)</td>
</tr>
<tr>
<td></td>
<td>4951.0 W / m²</td>
<td>459.5 W / ft.²</td>
</tr>
<tr>
<td>K</td>
<td>H_{D_{per h}} (J/I)</td>
<td>(J/I)</td>
</tr>
<tr>
<td></td>
<td>10271.8 W / m² / m</td>
<td>290.3 W / ft.² / ft.</td>
</tr>
<tr>
<td>L</td>
<td>H_{frame} -</td>
<td>-</td>
</tr>
<tr>
<td>M</td>
<td>n If Required: (L x K) / J</td>
<td>If Required: (L x K) / J</td>
</tr>
<tr>
<td></td>
<td>4.54 m</td>
<td>14.9 ft.</td>
</tr>
<tr>
<td>N</td>
<td>W_{add-horiz} If Required: [[[M+1] x H] / [L x (A+(B/2)+(C/2))] x K] x D</td>
<td>If Required: [[[M+1] x H] / [L x (A+(B/2)+(C/2))] x K] x D</td>
</tr>
</tbody>
</table>

Additional calculations for shelf-level equipment only

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>H_{shelf} 482.0 mm (0.482 m)</td>
<td>19.5 inches (1.583 ft.)</td>
</tr>
<tr>
<td>J</td>
<td>H_{D_{per shelf}} (H/G)</td>
<td>(H/G)</td>
</tr>
<tr>
<td></td>
<td>4951.0 W / m²</td>
<td>459.5 W / ft.²</td>
</tr>
<tr>
<td>K</td>
<td>H_{D_{per h}} (J/I)</td>
<td>(J/I)</td>
</tr>
<tr>
<td></td>
<td>10271.8 W / m² / m</td>
<td>290.3 W / ft.² / ft.</td>
</tr>
<tr>
<td>L</td>
<td>H_{frame} -</td>
<td>-</td>
</tr>
<tr>
<td>M</td>
<td>n If Required: (L x K) / J</td>
<td>If Required: (L x K) / J</td>
</tr>
</tbody>
</table>

**Major chassis components**

The major components in the Flex System Carrier-Grade chassis include 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 Carrier-Grade chassis:
Front view of the chassis

Compute nodes and the front panel LED card are in the front of the Flex System Carrier-Grade 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 without the airborne contaminant filter assembly.
Front information panel
The Flex System Carrier-Grade 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 915.

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 Carrier-Grade chassis.

The Flex System Carrier-Grade 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 Carrier-Grade 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 Carrier-Grade chassis, see http://www.lenovo.com/serverproven/.

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 Carrier-Grade 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.


**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 Carrier-Grade 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.

Warning: The intra-building port(s) (EN2092 I/O module Ethernet ports) of the equipment or subassembly are suitable for connection to intra-building or unexposed wiring or cabling only. The intra-building port(s) of the equipment or subassembly MUST NOT be metallically connected to interfaces that connect to the OSP or its wiring. These interfaces are designed for use as intra-building interfaces only (Type 2 or Type 4 ports as described in GR-1089) and require isolation from the exposed OSP cabling. The addition of Primary Protectors is not sufficient protection in order to connect these interfaces metallically to OSP wiring.

Attention: All CAT-5E cables used for the Flex System Carrier-Grade chassis must be shielded and grounded on both ends.

Notes: 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.

• To determine which I/O modules are compatible with the Flex System Carrier-Grade chassis, see [http://www.lenovo.com/serverproven/](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 Carrier-Grade chassis supports up to six autoranging power supplies.

The types of power supplies that are available for the Flex System Carrier-Grade chassis are listed in Table 5 “Chassis power supplies” on page 17.

<table>
<thead>
<tr>
<th>Rated output</th>
<th>Input voltage range</th>
<th>Power cord connector</th>
<th>FRU numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>2500 W</td>
<td>-48 to -60 V dc</td>
<td>2 position power connector</td>
<td>94Y8265</td>
</tr>
<tr>
<td>2500 W</td>
<td>200 to 240 V ac</td>
<td>C20</td>
<td>94Y8251 or 69Y5890</td>
</tr>
</tbody>
</table>
The power supplies get electrical power from either a -48 to -60 V dc power source or a 200 to 240 V ac power source, depending on the type of power supply. Both dc and ac-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 50 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 Carrier-Grade chassis. Mixing dc-powered supplies with ac-powered supplies in the same chassis is not supported. Each chassis must contain either all dc-powered supplies or all ac-powered supplies.

Notes: For ac-powered supplies:
• 200 - 208 VAC, 3-Phase Delta power distribution units (PDUs): The ac 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 ac 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.

<table>
<thead>
<tr>
<th>LED</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>DC power in (-48 to -60 V dc supplies only)</td>
<td><img src="https://example.com/IN.png" alt="IN" /> When this LED is lit (green), it indicates that dc power is being supplied to the power supply.</td>
</tr>
<tr>
<td>AC power in (200 - 240 V ac supplies only)</td>
<td><img src="https://example.com/IN.png" alt="IN" /> When this LED is lit (green), it indicates that ac power is being supplied to the power supply.</td>
</tr>
<tr>
<td>DC power out</td>
<td><img src="https://example.com/OUT.png" alt="OUT" /> When this LED is lit (green), it indicates that dc power is being supplied from the power supply to the chassis midplane.</td>
</tr>
<tr>
<td>Fault</td>
<td><img src="https://example.com/!" alt="!" /> When this LED is lit (yellow), it indicates that there is a fault in the power supply. Note: Before unplugging the 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.</td>
</tr>
</tbody>
</table>

Fan modules

The Flex System Carrier-Grade 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. The following is an illustration of the 80 mm fan modules:

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 39 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**

![Power-on LED](image)

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

**Fault LED**

![Fault LED](image)

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

**Fan logic modules**

The Flex System Carrier-Grade 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](image)

**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 Carrier-Grade chassis

Install the Flex System Carrier-Grade chassis in your facility by setting up and configuring all of the hardware components. The 11U Flex System Carrier-Grade chassis is suitable for installation in Network Telecommunication Facilities.

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.

Central Office (CO) environment

The Flex System Carrier-Grade chassis is ideally suited for network telecommunications facilities or carrier-grade environments that require maximum equipment operability. The Flex System Carrier-Grade chassisType 7385 (dc power) is intended to be installed in a Common Bonding Network (or mesh network) as described in GR-1089-CORE.

Special accessories required for installation

The Flex System Carrier-Grade chassis requires shielded CAT-5E cables grounded at both ends for all Ethernet port connections.

Statement 1

⚠️ DANGER

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

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

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

To Disconnect:

1. Turn everything OFF.
2. First, remove power cords from outlet.
3. Remove signal cables from connectors.
4. Remove all cables from devices.

Setting up your Flex System Carrier-Grade chassis

Follow the instructions in this section to set up the Flex System Carrier-Grade chassis hardware.

Before you begin, make the following preparations:

- Read “Safety” on page iii and “Handling static-sensitive devices” on page 936. 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 11 units of contiguous space (11U) is available in the rack.
- Connect an ESD wrist strap to the ESD connector on the Flex System Carrier-Grade chassis before removing or installing any components. See “Front view of the chassis” on page 11 and “Rear view of the chassis” on page 12 for the ESD connector locations.

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 24). You can also remove the chassis shelves to further reduce the weight.
2. Install the chassis in a rack (see “Installing the chassis in a rack” on page 29).
3. Reinstall all of the components that you removed (see “Installing components” on page 39).
4. Connect the chassis to earth ground. (see “Grounding the chassis” on page 48).
5. Cable the components in the chassis to the applicable external devices (see “Cabling the chassis” on page 50).
6. Connect the chassis to power (see “Connecting the chassis to power” on page 50).

Note: The Flex System Carrier-Grade chassis does not have a power switch. To turn off chassis power, see “Disconnecting the chassis from power” on page 55.

Removing components

Remove components to reduce the weight of the Flex System Carrier-Grade 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.

```
| ≥ 220.4 kg (488 lbs) | ≥ 66.2 kg (146 lbs) | ≥ 44.90 kg (99 lbs) |
```

**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 936.

b. Remove the airborne contaminant filter assembly, if one is installed. See “Removing the airborne contaminant filter assembly” on page 961 for instructions.

c. Remove all of the installed compute nodes.
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 960 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 both of the fan logic modules.
f. 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 Carrier-Grade 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 935.

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 Carrier-Grade 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 70 mm (2.76 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 access 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 936.

Step 2. Open the rail kit, the rack installation kit and the airborne contaminate filter 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:

- Fourteen M5 cage nuts (2 extra). Use on EIA flanges with square holes.
- Twenty-two M5 clip nuts (12 for rack installation, 8 for stand-alone installation, 2 extra). Use on EIA flanges with round holes.
- Ten M5x16 combi-head screws (black)
- One right rear support bracket
- One left rear support bracket
- One lower rear support bracket

The airborne contaminant filter assembly includes the following hardware:

- Two filter assembly mounting brackets (left and right)
- One filter assembly consisting of filter bezel with filter and filter retainer

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 37). 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.

Notes:

- Be sure to align the bottom edge of the chassis rail with the bottom U that you want the chassis to rest on. Be sure to align the bottom edge of the chassis rail 1U above 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 24 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 front of 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. 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 14a through 14c 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 bottom support bracket, two screws on the right side and two screws on the left side, but do not tighten the screws.

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

Step 15. Install the airborne contaminant filter mounting brackets on the front of the chassis:

   a. Align the left mounting bracket captive screws with the four empty screw holes on the left side of the chassis bezel. Thread the four captive screws through the bezel into the clip nuts to secure the left bracket to the chassis, but do not tighten the screws.

   b. Align the right mounting bracket captive screws with the four empty screw holes on the right side of the chassis bezel. Thread the four captive screws through the bezel into the clip nuts to secure the right bracket to the chassis, but do not tighten the screws.

   c. After all of the captive screws are installed, tighten the screws to 30 in-lbs (3.4 Nm) to secure the chassis to the rack.

Step 16. Reinstall the chassis shelves, if you removed them earlier.

Step 17. Reinstall the components (see “Installing components” on page 39).

Step 18. Install the airborne contaminate filter assembly on the front of the chassis:

   a. Insert the two hooks on the bottom of the filter assembly into the slots on the bottom of the chassis bezel.
b. Rotate the filter assembly toward the chassis by pushing on the front of the filter assembly until the slide latches click into place. Check the hooks on the bottom of the filter assembly to make sure that they are still in the slots on the bottom of the chassis.

Rack template
The rack template comes with the Flex System Carrier-Grade 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://pic.dhe.ibm.com/infocenter/flexsys/information/index.jsp?topic=%2Fcom.lenovo.acc.7385.doc%2Fprintable_doc.html
Screws required to secure rails before installing chassis

Note: 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.

Note: Make sure that there is sufficient room in front of the front rack rail to provide minimum bezel clearance of 70 mm (2.76 inches).

Note: If the rack rail has round holes, install the M5 clip nuts from the installation kit.

Note: An extra 1U of space is required below the chassis rail for the air duct on the bottom.

Note: An extra 1U of space is required below the chassis rail for the air duct on the bottom.

Note: If the rack rail has round holes, install the M5 clip nuts from the installation kit.
Installing components

After you install the Flex System Carrier-Grade chassis in a rack, install all of the components in the chassis.

Before you install components in the Flex System Carrier-Grade chassis:

- Read “Safety” on page iii and “Installation guidelines” on page 935.
- Make sure that the Chassis Management Module firmware is the latest level available. See "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 Carrier-Grade chassis, install them starting from the bottom up.

Compute nodes

The following illustration shows the locations of node bays in the Flex System Carrier-Grade chassis.

![Node Bay Locations](image)

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

Power supplies

The chassis power load is dependent on the number and type of compute 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 Power Configurator to determine the power load for a specific chassis configuration. See [http://www-03.ibm.com/systems/bladecenter/resources/powerconfig.html](http://www-03.ibm.com/systems/bladecenter/resources/powerconfig.html) for more information.

Important:
- Up to six power supplies can be installed.
• 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.

• Do not mix different types of power supplies in the Flex System Carrier-Grade chassis. Each chassis must contain either all dc-powered supplies or all ac-powered supplies.

Install power supplies according to the number of populated node bays as shown in Table 7 “Required power supplies relative to the number of populated node bays” on page 40. See also “Power supplies” on page 17 for more information.

**Table 7. Required power supplies relative to the number of populated node bays**

<table>
<thead>
<tr>
<th>Number of populated node bays</th>
<th>Power supplies required</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - 4</td>
<td>2</td>
</tr>
<tr>
<td>5 - 6</td>
<td>3</td>
</tr>
<tr>
<td>7 - 8</td>
<td>4</td>
</tr>
<tr>
<td>9 - 11</td>
<td>5</td>
</tr>
<tr>
<td>12 - 14</td>
<td>6</td>
</tr>
</tbody>
</table>

**80 mm fan modules**

The number of 80 mm fans that you install depends on the number of populated node bays. Up to eight 80 mm fan modules can be installed.

Install 80 mm fan modules according to the number of populated node bays as shown in Table 8 “Required 80 mm fan modules relative to the number of populated node bays” on page 40. See also “Fan modules” on page 19 for more information.

**Table 8. Required 80 mm fan modules relative to the number of populated node bays**

<table>
<thead>
<tr>
<th>Fan zone 1 (behind node bays 1, 3, 5, 7, 9, 11, and 13)</th>
<th>Fan zone 2 (behind node bays 2, 4, 6, 8, 10, 12, and 14)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of populated node bays</td>
<td>80 mm fans required</td>
</tr>
<tr>
<td>1 - 2</td>
<td>2</td>
</tr>
<tr>
<td>3 - 4</td>
<td>3</td>
</tr>
<tr>
<td>5 - 7</td>
<td>4</td>
</tr>
</tbody>
</table>

**Installing a 1-bay compute node**

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

Before you install a compute node in the Flex System Carrier-Grade chassis, complete the following steps:

1. Verify that the compute node is compatible with the chassis. See [http://www.lenovo.com/serverproven/](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 39 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 airborne contaminant filter assembly bezel, if one is installed (see “Removing the airborne contaminant filter assembly” on page 961).

**Note:** Remove only the airborne contaminant filter assembly bezel. You do not need to remove the filter assembly mounting brackets in order to install a compute node.

Step 2. 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 3. Open the release handle (rotate the handle to the left).

Step 4. Slide the compute node into the node bay until it is seated.

Step 5. Close the release handle (rotate the handle to the right).

After you install the compute node, complete the following steps:

1. Make a note of the compute node identification information on one of the labels that come with the Flex System Carrier-Grade chassis. Place a label on the node label tab. See “User labels” on page 54 for more information.

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

2. Install the airborne contaminant filter assembly bezel (see “Replacing the airborne contaminant filter assembly” on page 962).

**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 Carrier-Grade chassis, complete the following steps:

1. Verify that the compute node is compatible with the chassis. See [http://www.lenovo.com/serverproven/](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 39 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.

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

Step 1. Remove the airborne contaminant filter assembly bezel, if one is installed (see “Removing the airborne contaminant filter assembly” on page 961).

   **Note:** Remove only the airborne contaminant filter assembly bezel. You do not need to remove the filter assembly mounting brackets in order to install a compute node.

Step 2. Remove the node bay fillers, if they are installed. Push the filler release tab to the right; then, grasp the filler by the slot and pull it out of the bay.

Step 3. Remove the chassis shelf, if one is installed (see “Removing a chassis shelf” on page 960).

Step 4. Open both release handles (rotate the left handle to the left and rotate the right handle to the right).

Step 5. Slide the compute node into the node bays until it is seated.

Step 6. Close both release handles.

After you install the compute node, complete the following steps:

1. Make a note of the compute node identification information on one of the labels that come with the Flex System Carrier-Grade chassis. Place a label on the node label tab. See “User labels” on page 54 for more information.

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

2. Install the airborne contaminant filter assembly bezel (see “Replacing the airborne contaminant filter assembly” on page 962).

**Installing a Chassis Management Module**

You can install up to two Chassis Management Modules for redundancy support in the Flex System Carrier-Grade 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 14 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 see “Configuring the chassis by using the CMM” on page 59 for instructions.

**Installing a power supply**

The Flex System Carrier-Grade chassis comes with at least 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 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 Carrier-Grade chassis comes with at least 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 39 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 Carrier-Grade 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 onboard 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).

**Warning:** The intra-building port(s) (EN2092 I/O module Ethernet ports) of the equipment or subassembly are suitable for connection to intra-building or unexposed wiring or cabling only. The intra-building port(s) of the equipment or subassembly MUST NOT be metallically connected to interfaces that connect to the OSP or its wiring. These interfaces are designed for use as intra-building interfaces only (Type 2 or Type 4 ports as described in GR-1089) and require isolation from the exposed OSP cabling. The addition of Primary Protectors is not sufficient protection in order to connect these interfaces metallically to OSP wiring.

**Attention:** All CAT-5E cables used for the Flex System Carrier-Grade chassis must be shielded and grounded on both ends.

**Grounding the chassis**

Before connecting cables or powering the Flex System Carrier-Grade chassis, you must connect the chassis to earth ground.

**Statement 29**

![Warning Icon]

**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 34**

![Warning Icon]

**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 chassis equipped with -48 V dc power supplies:

<table>
<thead>
<tr>
<th>Breaker</th>
<th>Listed 70 A</th>
<th>See Note 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ground cable</td>
<td>4 AWG with Listed lug which can accept M6 ground screws</td>
<td>See Note 2</td>
</tr>
<tr>
<td>Torque rating for ground screws</td>
<td>4.0 - 4.8 Newton-meters (35.4 - 42.5 inch-pounds)</td>
<td>-</td>
</tr>
</tbody>
</table>

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 earth ground, complete the following steps:

1. Connect an earth ground cable to the ground studs on the rear of the chassis:

   - Use a 10 mm nut driver to remove the hex nuts from the ground studs.
   - Remove the lock washer and one of the flat washers from each ground stud.
c. 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.

d. Use a 10 mm nut driver to tighten the hex nuts to 4.0 - 4.8 Newton-meters (35.4 - 42.5 inch-pounds).

See “Cabling the chassis” on page 50 and “Connecting the chassis to power” on page 50 for more information.

Cabling the chassis

Cabling the Flex System Carrier-Grade 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.

**Warning:** The intra-building port(s) (EN2092 I/O module Ethernet ports) of the equipment or subassembly are suitable for connection to intra-building or unexposed wiring or cabling only. The intra-building port(s) of the equipment or subassembly MUST NOT be metallically connected to interfaces that connect to the OSP or its wiring. These interfaces are designed for use as intra-building interfaces only (Type 2 or Type 4 ports as described in GR-1089) and require isolation from the exposed OSP cabling. The addition of Primary Protectors is not sufficient protection in order to connect these interfaces metallically to OSP wiring.

**Attention:** All CAT-5E cables used for the Flex System Carrier-Grade chassis must be shielded and grounded on both ends.

Cabling to the network components in the Flex System Carrier-Grade 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.


See “Connecting the chassis to power” on page 50 for information about connecting the chassis power cords.

Connecting the chassis to power

Power is supplied to the Flex System Carrier-Grade 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 source. The Flex System Carrier-Grade chassis dc-power inputs are configured for dc isolated return (DC-I). The dc RETURN (RTN) terminal or conductor is not connected to the equipment frame or the grounding means of the equipment.

**Connecting for N+N power redundancy**

The Flex System Carrier-Grade 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 sources. 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 source 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 Carrier-Grade chassis does not have a power switch. See “Disconnecting the chassis from power” on page 55 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.

<table>
<thead>
<tr>
<th>To Connect:</th>
<th>To Disconnect:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Turn OFF all power sources and equipment that is to be attached to this product.</td>
<td>1. Turn OFF all power sources and equipment that is to be attached to this product.</td>
</tr>
<tr>
<td>2. Attach signal cables to the product.</td>
<td>• For ac systems, remove all power cords from the chassis power receptacles or interrupt power at the ac power distribution unit.</td>
</tr>
<tr>
<td>3. Attach power cords to the product.</td>
<td>• For dc systems, disconnect dc power sources at the breaker panel or by turning off the power source. Then, remove the dc cables.</td>
</tr>
<tr>
<td>• For ac systems, use appliance inlets.</td>
<td>2. Remove the signal cables from the connectors.</td>
</tr>
<tr>
<td>• 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.</td>
<td>3. Remove all cables from the devices.</td>
</tr>
<tr>
<td>4. Attach signal cables to other devices.</td>
<td></td>
</tr>
<tr>
<td>5. Connect power cords to their sources.</td>
<td></td>
</tr>
<tr>
<td>6. Turn ON all the power sources.</td>
<td></td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Breaker</th>
<th>List 70 A</th>
<th>See Note 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ground cable</td>
<td>4 AWG with Listed lug which can accept M6 ground screws</td>
<td>See Note 2</td>
</tr>
<tr>
<td>Torque rating for ground screws</td>
<td>4.0 - 4.8 Newton-meters (35.4 - 42.5 inch-pounds)</td>
<td>-</td>
</tr>
</tbody>
</table>

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 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 panel (PDP) (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 PDP only.

2. 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 Carrier-Grade 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.

3. Make sure that the following LEDs are lit:
   • The logo on the chassis front information panel.
   • The dc power in or ac power in and dc power out 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 Carrier-Grade chassis. Record the information to identify each installed compute node on the labels and place them on the node label tab. The large label (size 1) fits on the node label tabs.

**Important:** Do not place the label directly on the compute 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

Use the Chassis Management Module to update the chassis firmware.

The following chassis components have firmware that can be updated:

- Chassis Management Module
- Compute nodes
- I/O modules

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 Carrier-Grade chassis, update the Chassis Management Module firmware to the latest level available. See "Updating the CMM firmware" in the [Lenovo Flex System Chassis Management Module Installation Guide](http://flexsystem.lenovofiles.com/help/topic/com.lenovo.lxca.doc/aug_product_page.html) for more information.

### Using the Chassis Management Module


### Using the Lenovo XClarity Administrator

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.


### Disconnecting the chassis from power

Follow the instructions in this section to disconnect the Flex System Carrier-Grade chassis from all power sources.

Before you disconnect the Flex System Carrier-Grade chassis from power, be sure to follow these instructions to correctly shut down the compute nodes.
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.

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.
2. For ac systems, remove all power cords from the chassis power receptacles or interrupt power at the ac power distribution unit.
3. For dc systems, disconnect dc power sources at the breaker panel or by turning off the power source. Then, remove the dc cables.
4. Remove the signal cables from the connectors.
5. 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 chassis equipped with -48 V dc power supplies:

<table>
<thead>
<tr>
<th>Breaker</th>
<th>Listed 70 A</th>
<th>See Note 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ground cable</td>
<td>4 AWG with Listed lug which can accept M6 ground screws</td>
<td>See Note 2</td>
</tr>
<tr>
<td>Torque rating for ground screws</td>
<td>4.0 - 4.8 Newton-meters (35.4 - 42.5 inch-pounds)</td>
<td>-</td>
</tr>
</tbody>
</table>

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. 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 Carrier-Grade chassis

You can configure the Flex System Carrier-Grade chassis locally or remotely by using the Chassis Management Module web interface or by using the Lenovo XClarity Administrator, if one is available. You must use the CMM to create user accounts and to configure IP addresses for the CMM and the I/O modules. 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 Carrier-Grade 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 59).

   **Notes:**
   - Use the Chassis Management Module web interface to complete the chassis configuration.
   - If you have multiple chassis, you must establish user accounts and configure the IP addresses using the CMM for each chassis.

2. If a Lenovo XClarity Administrator is available, use the Lenovo XClarity Administrator to discover and configure the Flex System Carrier-Grade chassis (see “Configuring the chassis by using the Lenovo XClarity Administrator” on page 63).

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.

**Notes:**

- You must use the Chassis Management Module to establish user accounts and to configure IP addresses for the CMM and the I/O modules.
- If you have multiple chassis on the management network, you must establish user accounts and configure the IP addresses for each chassis.
- Use the Chassis Management Module web interface to complete the chassis configuration.


### CMM network access tag

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

**Important:** 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**

- DHCP is enabled by default
- MAC Address (Last 12 characters): MM↑↑↑↑↑↑↑↑↑↑↑↑
- Default Hostname: MM Label Here
- IPv6 Link Local Address (LLA): LLA Label Here

The rear 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**

- Default Information:
  - URL: https://192.168.70.100
  - User Name: USERID
  - Password: PASSW0RD

- Secure connection required.
  (e.g., SSH, https://, etc.)

**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:CB00.

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," 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 "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:

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 MMxxxxxxxxxxxx, where xxxxxxxxxx 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:

   - 00111001-A7-94-FF-FE-07-CB-D0
   - 00111011-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-CB00

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

   - 3BA7:94FF:FE07:CB00
   - 3BA7:94FF:FE07:CB00

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

   FE80::3BA7:94FF:FE07:CB00
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 MMxxxxxxxxxxxx, where xxxxxxxxxxxxx is the burned-in MAC address. The MAC address is on a label on the CMM, below the IP reset button (see “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 60 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. 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 Carrier-Grade 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 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 Carrier-Grade 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. To determine which I/O modules are compatible with the Flex System Carrier-Grade chassis, see http://www.lenovo.com/serverproven/.

Port mapping

Table 9 “I/O bay to expansion adapter port mapping” on page 63 summarizes the Flex System Carrier-Grade 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 9 “I/O bay to expansion adapter port mapping” on page 63 allows for dual paths from the compute node (or other device) to external devices.

Table 9. I/O bay to expansion adapter port mapping

<table>
<thead>
<tr>
<th>Chassis I/O bay</th>
<th>Compute node I/O expansion adapter port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Port 0 connection on the I/O expansion adapter in compute node position 1</td>
</tr>
<tr>
<td>2</td>
<td>Port 1 connection on the I/O expansion adapter in compute node position 1</td>
</tr>
<tr>
<td>3</td>
<td>Port 0 connection on the I/O expansion adapter in compute node position 2</td>
</tr>
<tr>
<td>4</td>
<td>Port 1 connection on the I/O expansion adapter in compute node position 2</td>
</tr>
</tbody>
</table>

The node in bay 1 in Figure 1 “LOM, I/O adapter, and network switch connections” on page 64 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 64.
A total of two I/O expansion adapters (M1 and M2 in Figure 2 “Logical layout of node-to-switch interconnections” on page 65) 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 65, 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.
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:** You must use the CMM to configure the compute nodes. See “Configuring the chassis by using the CMM” on page 59 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](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 Carrier-Grade chassis, see [http://www.lenovo.com/serverproven/](http://www.lenovo.com/serverproven/).
Chapter 4. Troubleshooting the chassis

If you experience problems with your Flex System Carrier-Grade chassis, there are several ways to isolate and solve the problem.

**Using the Lenovo XClarity Administrator**

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

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

**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 "service command" in the [Lenovo Flex System Chassis Management Module Command-Line Interface Reference Guide](http://datacentersupport.lenovo.com) for more information.

See also "Service and support options" in the [Lenovo Flex System Chassis Management Module User's Guide](http://datacentersupport.lenovo.com).

**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 Carrier-Grade chassis.

To find service bulletins that are available for the Flex System Carrier-Grade chassis, go to [http://datacentersupport.lenovo.com](http://datacentersupport.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 Carrier-Grade chassis.

You can view the Chassis Management Module event log by using the CMM command-line interface displaylog command or through the CMM web interface.

**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 Carrier-Grade 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” 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 10. Severity levels

<table>
<thead>
<tr>
<th>Severity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Informational</td>
<td>An informational message is information that is recorded for audit purposes, usually a user action or a change of states that is normal behavior.</td>
</tr>
<tr>
<td>Warning</td>
<td>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.</td>
</tr>
<tr>
<td>Error</td>
<td>An error typically indicates a failure or critical condition that impairs service or an expected function.</td>
</tr>
</tbody>
</table>

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 915 and “Chassis module LEDs” on page 917.

**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.

<table>
<thead>
<tr>
<th>Alert categories</th>
<th>MIB object</th>
<th>Object identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Critical/Error</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chassis/System Management (Critical)</td>
<td>mmTrapChassisC</td>
<td>1.3.6.1.4.1.2.6.158.3.0.130</td>
</tr>
<tr>
<td>Cooling devices (Critical)</td>
<td>mmTrapFanC</td>
<td>1.3.6.1.4.1.2.6.158.3.0.133</td>
</tr>
<tr>
<td>Power supplies (Critical)</td>
<td>mmTrapPsC</td>
<td>1.3.6.1.4.1.2.6.158.3.0.4</td>
</tr>
<tr>
<td>Nodes (Critical)</td>
<td>mmTrapBladeC</td>
<td>1.3.6.1.4.1.2.6.158.3.0.128</td>
</tr>
<tr>
<td>I/O modules (Critical)</td>
<td>mmTrapIOC</td>
<td>1.3.6.1.4.1.2.6.158.3.0.129</td>
</tr>
<tr>
<td>Storage modules (Critical)</td>
<td>mmTrapStorageC</td>
<td>1.3.6.1.4.1.2.6.158.3.0.131</td>
</tr>
<tr>
<td><strong>NonCritical/Warning</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chassis/System Management (Warning)</td>
<td>mmTrapChassisN</td>
<td>1.3.6.1.4.1.2.6.158.3.0.162</td>
</tr>
<tr>
<td>Cooling devices (Warning)</td>
<td>mmTrapFanN</td>
<td>1.3.6.1.4.1.2.6.158.3.0.165</td>
</tr>
</tbody>
</table>
### Alert categories

<table>
<thead>
<tr>
<th>Alert categories</th>
<th>MIB object</th>
<th>Object identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power supplies (Warning)</td>
<td>mmTrapPowerN</td>
<td>.1.3.6.1.4.1.2.6.158.3.0.164</td>
</tr>
<tr>
<td>Nodes (Warning)</td>
<td>mmTrapBladeN</td>
<td>.1.3.6.1.4.1.2.6.158.3.0.160</td>
</tr>
<tr>
<td>I/O modules (Warning)</td>
<td>mmTrapION</td>
<td>.1.3.6.1.4.1.2.6.158.3.0.161</td>
</tr>
<tr>
<td>Storage Modules (Warning)</td>
<td>mmTrapStorageN</td>
<td>.1.3.6.1.4.1.2.6.158.3.0.163</td>
</tr>
<tr>
<td>Event Log (Warning)</td>
<td>mmTrapLogFullN</td>
<td>.1.3.6.1.4.1.2.6.158.3.0.7</td>
</tr>
</tbody>
</table>

#### System/Informational

<table>
<thead>
<tr>
<th>Chassis/System Management (Informational)</th>
<th>mmTrapChassisS</th>
<th>.1.3.6.1.4.1.2.6.158.3.0.178</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cooling devices (Informational)</td>
<td>mmTrapFanS</td>
<td>.1.3.6.1.4.1.2.6.158.3.0.181</td>
</tr>
<tr>
<td>Power supplies (Informational)</td>
<td>mmTrapPowerS</td>
<td>.1.3.6.1.4.1.2.6.158.3.0.180</td>
</tr>
<tr>
<td>Nodes (Informational)</td>
<td>mmTrapBladeS</td>
<td>.1.3.6.1.4.1.2.6.158.3.0.176</td>
</tr>
<tr>
<td>I/O modules (Informational)</td>
<td>mmTrapIOS</td>
<td>.1.3.6.1.4.1.2.6.158.3.0.177</td>
</tr>
<tr>
<td>Storage modules (Informational)</td>
<td>mmTrapStorageS</td>
<td>.1.3.6.1.4.1.2.6.158.3.0.179</td>
</tr>
<tr>
<td>Event log (Informational)</td>
<td>mmTrapSysLogS</td>
<td>.1.3.6.1.4.1.2.6.158.3.0.35</td>
</tr>
<tr>
<td>Power on/off (Informational)</td>
<td>mmTrapPwrDOS</td>
<td>.1.3.6.1.4.1.2.6.158.3.0.182</td>
</tr>
<tr>
<td>Inventory change (Informational)</td>
<td>mmTrapSysInvS</td>
<td>.1.3.6.1.4.1.2.6.158.3.0.34</td>
</tr>
<tr>
<td>Network change (Informational)</td>
<td>mmTrapNwChangeS</td>
<td>.1.3.6.1.4.1.2.6.158.3.0.37</td>
</tr>
<tr>
<td>User activity (Informational)</td>
<td>mmTrapRemoteLoginS</td>
<td>.1.3.6.1.4.1.2.6.158.3.0.30</td>
</tr>
<tr>
<td>Test message</td>
<td>mmTrapAppS</td>
<td>.1.3.6.1.4.1.2.6.158.3.0.22</td>
</tr>
</tbody>
</table>

#### 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://datacentersupport.lenovo.com](http://datacentersupport.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.

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.
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.


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.
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
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.

- **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.

- **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 disabled the specified chassis internal network (CIN) node pair.
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.

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.
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.

  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.

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

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**

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.

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)
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

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.

   • 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.

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.

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
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

I/O Modules (Informational)

SNMP Trap ID

mmTrapIOS

CIM Information

Prefix: CMM ID: 0070

User Response

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

Severity

Informational

Serviceable

Yes

Automatically notify support

No

Alert Category

Nodes (Informational)

SNMP Trap ID

mmTrapBladeS

CIM Information

Chapter 4. Troubleshooting the chassis 95
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.

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.


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.


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.

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.


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.


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.
Alert Category
Nodes (Informational)

SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM ID: 0743

User Response
Information only; no action is required.


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.


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)
• **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

118  Lenovo Flex System Carrier-Grade chassis Installation and Service Guide
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
• 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
00016020: Account password will expire for user [arg1] in [arg2] days.

The password for the specified user account will expire within 7 days.

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.
• 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
mm TrapRemoteLoginS
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
mm TrapRemoteLoginS
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
mm TrapRemoteLoginS
CIM Information
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
Chapter 4. Troubleshooting the chassis 129
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.


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.
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.


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.
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.

   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.


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.


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.

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 address 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
• 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: 0204

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: 0205

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 account [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.

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.

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.

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.

  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.

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.

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.


  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**
• **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.


  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
• **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.

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.

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.


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.

  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
• 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
• **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

• 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).
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.


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 recommended 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
• 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
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
• **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.

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.

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.


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.


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.


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.


  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.


  The specified user has changed the node bay data for the specified node.
CIM Information
Prefix: CMM ID: 0565

User Response
Information only; no action is required.


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.


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.


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.
User Response
  Information only; no action is required.


  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.


  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.


  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.


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.


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.


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.

  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.


  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.


  The specified user has changed the port number of the LDAP client to connect to an LDAP server.
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.

  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 committed VLAN configuration.
  The VLAN temporary commit timeout has expired. Reverted to the last committed 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.


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.


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.


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.

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.


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.


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.


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.


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.
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
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.
User Response
Information only; no action is required.

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.

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.

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.

  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.

  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.

  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
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

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
• 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.
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
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


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

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
- **00016807**: Service data collection completed on CMM [arg1].

  Service data collection completed on specified CMM.

  **Severity**
  Informational

  **Serviceable**
  No

  **Automatically notify support**
  No

- **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: 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 the 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.


  The specified user has uploaded a file to the Chassis Management Module.
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**
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
Ethernet host name changed.

User acknowledged an alarm in the alarm list.

User 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
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

User Response
Information only; no action is required.

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

User Response
Information only; no action is required.

The user created software event with a given severity and text.

Severity
Warning

Serviceable
No

Automatically notify support
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
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

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

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
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

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

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**
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).
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
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
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**

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**

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
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

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

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.
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.
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.
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.
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.
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.
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**
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**
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.
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**
mnTrapChassisN

**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**
mnTrapChassisN

**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
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.
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.
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.

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.
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.
• **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.

- **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.

- **000A2202** : 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.
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.
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
• 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)\(^1\)**

**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.
SNMP Trap ID
  mmTrapRemoteLoginS

CIM Information
  Prefix: CMM ID: 0755

User Response
  Information only; no action is required.


  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.


  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.


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.


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.


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
• 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

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

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.
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
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:** 0250

**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.
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.
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: 0256

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.
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.
• **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**
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.
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**
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.


  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.

- **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.

- **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.
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.
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.
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
• **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
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
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.
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**
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  
mnTrapPsC

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  
mnTrapPsC

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  
mnTrapPsC

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

- **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

- **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**
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.
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

User Response
At the next scheduled maintenance opportunity, replace the specified 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

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

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.
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)

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)

0901E003 : Chassis rear LED card not present.

Install or replace the front LED card. Make sure that the front LED card is connected after a maintenance action.
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.
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.
CIM Information
Prefix: CMM ID: 0103

User Response
Information only; no action is required.

• **OA002106** : 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.

• **OA002107** : 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.

• **OA002108** : 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
• 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.
• OE00200D: 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.

• OE00200E: 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.

• OE002101: 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.
• **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

---

• **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**
- mmTrapSyInvS

---

• **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
**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.
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.

- **OE006009 : 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.

- **OE00600A : 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.

- **OE00600B : 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.
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.

• **OE00600E** : 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
UserResponse

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

UserResponse

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

Chapter 4. Troubleshooting the chassis 513
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.
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
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
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: 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.

- **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.

• OE010004: 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.

• OE010005: 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

Chapter 4. Troubleshooting the chassis 527
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
User Response

Information only; no action is required.

- **OE020008** : 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.

- **OE020009** : 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.

- **OE02000A** : 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.

- OE02000B: 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.

- OE02000C: 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.
SNMP Trap ID
mmTrapBladeS

CIM Information
Prefix: CMM ID: 0747

User Response
Information only; no action is required.

- **OE02000D** : 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.

- **OE02000E** : 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.

<table>
<thead>
<tr>
<th><strong>Severity</strong></th>
<th>Warning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Serviceable</strong></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Automatically notify support</strong></td>
<td>No</td>
</tr>
<tr>
<td><strong>Alert Category</strong></td>
<td>Nodes (Warning)</td>
</tr>
<tr>
<td><strong>SNMP Trap ID</strong></td>
<td>mmTrapBladeN</td>
</tr>
<tr>
<td><strong>CIM Information</strong></td>
<td>Prefix: CMM ID: 0170</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th><strong>Severity</strong></th>
<th>Warning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Serviceable</strong></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Automatically notify support</strong></td>
<td>No</td>
</tr>
<tr>
<td><strong>Alert Category</strong></td>
<td>Nodes (Warning)</td>
</tr>
<tr>
<td><strong>SNMP Trap ID</strong></td>
<td>mmTrapBladeN</td>
</tr>
<tr>
<td><strong>CIM Information</strong></td>
<td>Prefix: CMM ID: 0170</td>
</tr>
</tbody>
</table>

**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.

- **OE200005**: 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.

- **OE200006**: 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.

- **OE200009 : 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.

- **OE20000A : 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**
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**
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.

- OEA04004 : 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.

- OEA06001 : 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.
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: 0689

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: 0689
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.
• OEA0A004 : 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.

• OEA0C001 : 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).

• OEA0C002 : 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.
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

- **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.

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.

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.

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.

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.
• 0EAO0D901 : 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.
**User Response**
Retry the I/O Module firmware activation a few minutes after the initial 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.


  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 initial 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.


  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
• 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 initial 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.

- **0E0A0ED03** : 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.

- **0E0A0ED04** : 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.

- **0E0AF101** : 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.

• OEA0F102 : 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.

• OEA0F103 : I/O module [arg1] enabled Protected Mode control of IP configuration.

I/O module specified enabled Protected Mode control of IP configuration.
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: 0426

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.

- **0E0A0F504**: 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.

- **0E0A0F601**: 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.

- **0E0A0F602**: 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.
Prefix: CMM ID: 0432

User Response
Information only; no action is required.

- OEA0FE04 : 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.

- OEA12001 : 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.

- OEA12002 : 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.

- **0E1A2003**: 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.

- **0E1A2004**: 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
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.
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.

- OEA15003 : 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.

- OEA15004 : 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.

- OEA17001 : 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.
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.
SNMP Trap ID
mmTrapIOS

CIM Information
Prefix: CMM ID: 0682

User Response
Information only; no action is required.

• OEA1C001: 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.

• OEA1C002: 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.

• OEA1C003: 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.
• OEAI04 : 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.

• 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.
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 initial 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 initial 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**
User Response
Retry the I/O Module service data collection a few minutes after the initial 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 initial 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
The specified I/O module powered on.

- **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 firmware 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 firmware 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.


  The specified firmware 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.


  The specified firmware image was set to be delay activated by the specified user.
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 firmware 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 initial 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 firmware 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 initial 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 firmware 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 initial 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 firmware 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 initial 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.
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
• 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 propriety management configuration a few minutes after the initial 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 propriety management configuration a few minutes after the initial 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 propriety management configuration a few minutes after the initial 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 proprietary management configuration a few minutes after the initial 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 proprietary 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.
User Response
Retry the I/O Module internal proprietary 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 proprietary 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 proprietary 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.
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.

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.
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.
• **0E2E004**: 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.
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)
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**
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

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

Chassis Management Module detected that Fabric Manager could not be applied to one or more devices at the specified node.
• OF00B008 : 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.

• OF00B009 : 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.

• OF00B00A : 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
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

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.
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-management 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-management 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 cannot be powered on because the Chassis Management Module will not grant permission to power on to the system-management 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 cannot be powered on because the Chassis Management Module will not grant permission to power on to the system-management processor on the node.

Severity
Warning

Serviceable
Yes

Automatically notify support
No

Alert Category
Nodes (Warning)
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-management processor on the node.

### Severity
Warning

### Serviceable
Yes

### Automatically notify support
No

### Alert Category
Nodes (Warning)

### SNMP Trap ID
mmTrapBladeN

### 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-management 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

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-management 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-management 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-management 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-management 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-management 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-management 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 cannot be powered on because the Chassis Management Module will not grant permission to power on to the system-management 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 cannot be powered on because the Chassis Management Module will not grant permission to power on to the system-management 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-management processor on the node.

**Severity**
Warning

**Serviceable**
No

**Automatically notify support**
No

**Alert Category**
Nodes (Warning)

**SNMP Trap ID**
mnTrapBladeN

**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-management processor on the node.

**Severity**
Warning

**Serviceable**
No

**Automatically notify support**
No

**Alert Category**
Nodes (Warning)

**SNMP Trap ID**
mnTrapBladeN

**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-management 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 cannot be powered on because the Chassis Management Module will not grant permission to power on to the system-management 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 cannot be powered on because the Chassis Management Module will not grant permission to power on to the system-management 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-management 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-management processor on the node.

Severity
Warning

Serviceable
No

Automatically notify support
No

Alert Category
Nodes (Warning)

SNMP Trap ID
mmTrapBladeN

CIM Information
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-management 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-management 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-management 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-management 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-management processor on the node.
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-management 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-management processor on the node.
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.
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
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.

- **OF010203**: 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.

- **OF010204**: 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.
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.
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
• **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.
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.
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
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.
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.

- \textbf{1E00E00C:} Fabric Manager configuration mismatch detected between the expected configuration and the actual configuration of node \[\text{arg1}\]. 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.

- \textbf{1E00E00D:} Fabric Manager configuration mismatch detected between the expected configuration and the actual configuration of node \[\text{arg1}\]. 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
Chapter 4. Troubleshooting the chassis

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**
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
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.
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.

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.
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.
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)
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)

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)

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.
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.

  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.

  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.

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.
• **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

**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**
mnTrapBladeS

**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
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.

Severi

Informational

Serviceable

No

Automatically notify support

No

Alert Category

Nodes (Informational)
• **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**
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.
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
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
• **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**
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)
• **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.
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.

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.**

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.

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.**
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**
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 into 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.
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.
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
• **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.
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.

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.
**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
• **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**  

• **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 node [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**
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
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**
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.
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
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.
• **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: 0926

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.


  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
• **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.


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] 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] 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
• **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

---

• **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.
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.
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.

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**
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.


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
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.
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**
mTrapRemoteLoginS

**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**
mTrapRemoteLoginS

**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**
mTrapChassisC

**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.
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.
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
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

---

**Chapter 4. Troubleshooting the chassis 879**
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**
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

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.


  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
**User Response**

Information only; no action is required.


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
• **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**
mnTrapRemoteLoginS

**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**
mnTrapSysInvS

**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 11. Events that automatically notify Support

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Message String</th>
<th>Automatically Notify Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>00006011</td>
<td>The battery in Chassis Management Module [arg1] is low.</td>
<td>Yes</td>
</tr>
<tr>
<td>00006012</td>
<td>The battery in Chassis Management Module [arg1] is low.</td>
<td>Yes</td>
</tr>
<tr>
<td>00006120</td>
<td>Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>00006121</td>
<td>Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>00006122</td>
<td>Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>00006123</td>
<td>Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>00006124</td>
<td>Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>00006125</td>
<td>Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>00006126</td>
<td>Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>00006220</td>
<td>Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>00006221</td>
<td>Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>00006222</td>
<td>Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>00006223</td>
<td>Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>00006224</td>
<td>Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>00006225</td>
<td>Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>00006226</td>
<td>Chassis Management Module [arg1] failure. FPGA Host [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>00016802</td>
<td>Test call home by user ID [arg1] from [arg2] at IP address [arg3].</td>
<td>Yes</td>
</tr>
<tr>
<td>00017104</td>
<td>CMM bay location cannot be determined, defaulting to CMM bay 2.</td>
<td>Yes</td>
</tr>
<tr>
<td>00022003</td>
<td>Primary Chassis Management Module real-time clock failed.</td>
<td>Yes</td>
</tr>
<tr>
<td>0002200A</td>
<td>Primary Chassis Management Module internal Ethernet logic failed.</td>
<td>Yes</td>
</tr>
<tr>
<td>00022015</td>
<td>Standby Chassis Management Module real-time clock failed.</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Table 11. Events that automatically notify Support (continued)

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Message String</th>
<th>Automatically Notify Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>00022016</td>
<td>Standby Chassis Management Module local management bus failed.</td>
<td>Yes</td>
</tr>
<tr>
<td>00022019</td>
<td>Standby Chassis Management Module internal I/O logic failure.</td>
<td>Yes</td>
</tr>
<tr>
<td>0002201D</td>
<td>Standby Chassis Management Module internal Ethernet logic failed.</td>
<td>Yes</td>
</tr>
<tr>
<td>0002201E</td>
<td>Standby Chassis Management Module communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>0002205A</td>
<td>Primary Chassis Management Module internal I/O logic failure.</td>
<td>Yes</td>
</tr>
<tr>
<td>00026801</td>
<td>Fan module [arg1] has failed.</td>
<td>Yes</td>
</tr>
<tr>
<td>00026802</td>
<td>Fan module [arg1] has failed.</td>
<td>Yes</td>
</tr>
<tr>
<td>00026803</td>
<td>Fan module [arg1] has failed.</td>
<td>Yes</td>
</tr>
<tr>
<td>00026804</td>
<td>Fan module [arg1] has failed.</td>
<td>Yes</td>
</tr>
<tr>
<td>00026805</td>
<td>Fan module [arg1] has failed.</td>
<td>Yes</td>
</tr>
<tr>
<td>00026806</td>
<td>Fan module [arg1] has failed.</td>
<td>Yes</td>
</tr>
<tr>
<td>00026807</td>
<td>Fan module [arg1] has failed.</td>
<td>Yes</td>
</tr>
<tr>
<td>00026808</td>
<td>Fan module [arg1] has failed.</td>
<td>Yes</td>
</tr>
<tr>
<td>00026809</td>
<td>Fan module [arg1] has failed.</td>
<td>Yes</td>
</tr>
<tr>
<td>0002680A</td>
<td>Fan module [arg1] has failed.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038201</td>
<td>Power supply [arg1] transient reading overvoltage.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038202</td>
<td>Power supply [arg1] transient reading overvoltage.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038203</td>
<td>Power supply [arg1] transient reading overvoltage.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038204</td>
<td>Power supply [arg1] transient reading overvoltage.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038205</td>
<td>Power supply [arg1] transient reading overvoltage.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038206</td>
<td>Power supply [arg1] transient reading overvoltage.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038301</td>
<td>Power supply [arg1] transient reading undervoltage.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038302</td>
<td>Power supply [arg1] transient reading undervoltage.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038303</td>
<td>Power supply [arg1] transient reading undervoltage.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038304</td>
<td>Power supply [arg1] transient reading undervoltage.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038305</td>
<td>Power supply [arg1] transient reading undervoltage.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038306</td>
<td>Power supply [arg1] transient reading undervoltage.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038401</td>
<td>Power supply [arg1] transient reading overcurrent.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038402</td>
<td>Power supply [arg1] transient reading overcurrent.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038403</td>
<td>Power supply [arg1] transient reading overcurrent.</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Table 11. Events that automatically notify Support (continued)

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Message String</th>
<th>Automatically Notify Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>00038404</td>
<td>Power supply [arg1] transient reading overcurrent.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038405</td>
<td>Power supply [arg1] transient reading overcurrent.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038406</td>
<td>Power supply [arg1] transient reading overcurrent.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038501</td>
<td>Power supply [arg1] power meter is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038502</td>
<td>Power supply [arg1] power meter is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038503</td>
<td>Power supply [arg1] power meter is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038504</td>
<td>Power supply [arg1] power meter is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038505</td>
<td>Power supply [arg1] power meter is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038506</td>
<td>Power supply [arg1] power meter is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038601</td>
<td>Fan module [arg1] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038602</td>
<td>Fan module [arg1] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038603</td>
<td>Fan module [arg1] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038604</td>
<td>Fan module [arg1] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038605</td>
<td>Fan module [arg1] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038606</td>
<td>Fan module [arg1] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038607</td>
<td>Fan module [arg1] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038608</td>
<td>Fan module [arg1] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038609</td>
<td>Fan module [arg1] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>0003860A</td>
<td>Fan module [arg1] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038701</td>
<td>Fan logic module [arg1] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038702</td>
<td>Fan logic module [arg1] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038A01</td>
<td>Power supply [arg1] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038A02</td>
<td>Power supply [arg1] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038A03</td>
<td>Power supply [arg1] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038A04</td>
<td>Power supply [arg1] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038A05</td>
<td>Power supply [arg1] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038A06</td>
<td>Power supply [arg1] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038F01</td>
<td>Internal proprietary management protocol between I/O module [arg1] and CMM is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038F02</td>
<td>Internal proprietary management protocol between I/O module [arg1] and CMM is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038F03</td>
<td>Internal proprietary management protocol between I/O module [arg1] and CMM is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>00038F04</td>
<td>Internal proprietary management protocol between I/O module [arg1] and CMM is offline.</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Table 11. Events that automatically notify Support (continued)

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Message String</th>
<th>Automatically Notify Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>00039601</td>
<td>Fan module [arg1] VPD is not available.</td>
<td>Yes</td>
</tr>
<tr>
<td>00039602</td>
<td>Fan module [arg1] VPD is not available.</td>
<td>Yes</td>
</tr>
<tr>
<td>00039603</td>
<td>Fan module [arg1] VPD is not available.</td>
<td>Yes</td>
</tr>
<tr>
<td>00039604</td>
<td>Fan module [arg1] VPD is not available.</td>
<td>Yes</td>
</tr>
<tr>
<td>00039605</td>
<td>Fan module [arg1] VPD is not available.</td>
<td>Yes</td>
</tr>
<tr>
<td>00039606</td>
<td>Fan module [arg1] VPD is not available.</td>
<td>Yes</td>
</tr>
<tr>
<td>00039607</td>
<td>Fan module [arg1] VPD is not available.</td>
<td>Yes</td>
</tr>
<tr>
<td>00039608</td>
<td>Fan module [arg1] VPD is not available.</td>
<td>Yes</td>
</tr>
<tr>
<td>00039609</td>
<td>Fan module [arg1] VPD is not available.</td>
<td>Yes</td>
</tr>
<tr>
<td>0003960A</td>
<td>Fan module [arg1] VPD is not available.</td>
<td>Yes</td>
</tr>
<tr>
<td>00039701</td>
<td>Fan logic module [arg1] VPD is not available.</td>
<td>Yes</td>
</tr>
<tr>
<td>00039702</td>
<td>Fan logic module [arg1] VPD is not available.</td>
<td>Yes</td>
</tr>
<tr>
<td>00039A01</td>
<td>Power supply [arg1] VPD is not available.</td>
<td>Yes</td>
</tr>
<tr>
<td>00039A02</td>
<td>Power supply [arg1] VPD is not available.</td>
<td>Yes</td>
</tr>
<tr>
<td>00039A03</td>
<td>Power supply [arg1] VPD is not available.</td>
<td>Yes</td>
</tr>
<tr>
<td>00039A04</td>
<td>Power supply [arg1] VPD is not available.</td>
<td>Yes</td>
</tr>
<tr>
<td>00039A05</td>
<td>Power supply [arg1] VPD is not available.</td>
<td>Yes</td>
</tr>
<tr>
<td>00039A06</td>
<td>Power supply [arg1] VPD is not available.</td>
<td>Yes</td>
</tr>
<tr>
<td>00039B01</td>
<td>Fan module [arg1] fan parameter in VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>00039B02</td>
<td>Fan module [arg1] fan parameter in VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>00039B03</td>
<td>Fan module [arg1] fan parameter in VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>00039B04</td>
<td>Fan module [arg1] fan parameter in VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>00039B05</td>
<td>Fan module [arg1] fan parameter in VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>00039B06</td>
<td>Fan module [arg1] fan parameter in VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>00039B07</td>
<td>Fan module [arg1] fan parameter in VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>00039B08</td>
<td>Fan module [arg1] fan parameter in VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>00039B09</td>
<td>Fan module [arg1] fan parameter in VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>00039BOA</td>
<td>Fan module [arg1] fan parameter in VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>000A2101</td>
<td>Fan logic module [arg1] has failed.</td>
<td>Yes</td>
</tr>
<tr>
<td>000A2102</td>
<td>Fan logic module [arg1] has failed.</td>
<td>Yes</td>
</tr>
<tr>
<td>000A2201</td>
<td>Fan logic module [arg1] is an older revision card (FRU 81Y2912) and needs to be replaced.</td>
<td>Yes</td>
</tr>
<tr>
<td>000A2202</td>
<td>Fan logic module [arg1] is an older revision card (FRU 81Y2912) and needs to be replaced.</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Table 11. Events that automatically notify Support (continued)

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Message String</th>
<th>Automatically Notify Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>000A6001</td>
<td>Fan module [arg1] is operating in a degraded state.</td>
<td>Yes</td>
</tr>
<tr>
<td>000A6002</td>
<td>Fan module [arg1] is operating in a degraded state.</td>
<td>Yes</td>
</tr>
<tr>
<td>000A6003</td>
<td>Fan module [arg1] is operating in a degraded state.</td>
<td>Yes</td>
</tr>
<tr>
<td>000A6004</td>
<td>Fan module [arg1] is operating in a degraded state.</td>
<td>Yes</td>
</tr>
<tr>
<td>000A6005</td>
<td>Fan module [arg1] is operating in a degraded state.</td>
<td>Yes</td>
</tr>
<tr>
<td>000A6006</td>
<td>Fan module [arg1] is operating in a degraded state.</td>
<td>Yes</td>
</tr>
<tr>
<td>000A6007</td>
<td>Fan module [arg1] is operating in a degraded state.</td>
<td>Yes</td>
</tr>
<tr>
<td>000A6008</td>
<td>Fan module [arg1] is operating in a degraded state.</td>
<td>Yes</td>
</tr>
<tr>
<td>000A6009</td>
<td>Fan module [arg1] is operating in a degraded state.</td>
<td>Yes</td>
</tr>
<tr>
<td>000A600A</td>
<td>Fan module [arg1] is operating in a degraded state.</td>
<td>Yes</td>
</tr>
<tr>
<td>08028001</td>
<td>Power supply [arg1] is off. DC fault.</td>
<td>Yes</td>
</tr>
<tr>
<td>08028002</td>
<td>Power supply [arg1] is off. DC fault.</td>
<td>Yes</td>
</tr>
<tr>
<td>08028003</td>
<td>Power supply [arg1] is off. DC fault.</td>
<td>Yes</td>
</tr>
<tr>
<td>08028004</td>
<td>Power supply [arg1] is off. DC fault.</td>
<td>Yes</td>
</tr>
<tr>
<td>08028005</td>
<td>Power supply [arg1] is off. DC fault.</td>
<td>Yes</td>
</tr>
<tr>
<td>08028006</td>
<td>Power supply [arg1] is off. DC fault.</td>
<td>Yes</td>
</tr>
<tr>
<td>08200001</td>
<td>Power supply [arg1] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>08200002</td>
<td>Power supply [arg1] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>08200003</td>
<td>Power supply [arg1] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>08200004</td>
<td>Power supply [arg1] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>08200005</td>
<td>Power supply [arg1] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>08200006</td>
<td>Power supply [arg1] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>08216301</td>
<td>Mismatched power supplies in the chassis: [arg1]. The configuration is not supported.</td>
<td>Yes</td>
</tr>
<tr>
<td>08236001</td>
<td>Power supply [arg1] has shut down because of an overcurrent fault.</td>
<td>Yes</td>
</tr>
<tr>
<td>08236002</td>
<td>Power supply [arg1] has shut down because of an overcurrent fault.</td>
<td>Yes</td>
</tr>
<tr>
<td>08236003</td>
<td>Power supply [arg1] has shut down because of an overcurrent fault.</td>
<td>Yes</td>
</tr>
<tr>
<td>08236004</td>
<td>Power supply [arg1] has shut down because of an overcurrent fault.</td>
<td>Yes</td>
</tr>
<tr>
<td>08236005</td>
<td>Power supply [arg1] has shut down because of an overcurrent fault.</td>
<td>Yes</td>
</tr>
<tr>
<td>08236006</td>
<td>Power supply [arg1] has shut down because of an overcurrent fault.</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Table 11. Events that automatically notify Support (continued)

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Message String</th>
<th>Automatically Notify Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>08236481</td>
<td>Power supply [arg1] has shut down because of an overvoltage fault.</td>
<td>Yes</td>
</tr>
<tr>
<td>08236482</td>
<td>Power supply [arg1] has shut down because of an overvoltage fault.</td>
<td>Yes</td>
</tr>
<tr>
<td>08236483</td>
<td>Power supply [arg1] has shut down because of an overvoltage fault.</td>
<td>Yes</td>
</tr>
<tr>
<td>08236484</td>
<td>Power supply [arg1] has shut down because of an overvoltage fault.</td>
<td>Yes</td>
</tr>
<tr>
<td>08236485</td>
<td>Power supply [arg1] has shut down because of an overvoltage fault.</td>
<td>Yes</td>
</tr>
<tr>
<td>08236486</td>
<td>Power supply [arg1] has shut down because of an overvoltage fault.</td>
<td>Yes</td>
</tr>
<tr>
<td>08236801</td>
<td>Power supply [arg1] has shut down because of an undervoltage fault.</td>
<td>Yes</td>
</tr>
<tr>
<td>08236802</td>
<td>Power supply [arg1] has shut down because of an undervoltage fault.</td>
<td>Yes</td>
</tr>
<tr>
<td>08236803</td>
<td>Power supply [arg1] has shut down because of an undervoltage fault.</td>
<td>Yes</td>
</tr>
<tr>
<td>08236804</td>
<td>Power supply [arg1] has shut down because of an undervoltage fault.</td>
<td>Yes</td>
</tr>
<tr>
<td>08236805</td>
<td>Power supply [arg1] has shut down because of an undervoltage fault.</td>
<td>Yes</td>
</tr>
<tr>
<td>08236806</td>
<td>Power supply [arg1] has shut down because of an undervoltage fault.</td>
<td>Yes</td>
</tr>
<tr>
<td>08526001</td>
<td>Power supply [arg1] encountered an internal fan failure.</td>
<td>Yes</td>
</tr>
<tr>
<td>08526002</td>
<td>Power supply [arg1] encountered an internal fan failure.</td>
<td>Yes</td>
</tr>
<tr>
<td>08526003</td>
<td>Power supply [arg1] encountered an internal fan failure.</td>
<td>Yes</td>
</tr>
<tr>
<td>08526004</td>
<td>Power supply [arg1] encountered an internal fan failure.</td>
<td>Yes</td>
</tr>
<tr>
<td>08526005</td>
<td>Power supply [arg1] encountered an internal fan failure.</td>
<td>Yes</td>
</tr>
<tr>
<td>08526006</td>
<td>Power supply [arg1] encountered an internal fan failure.</td>
<td>Yes</td>
</tr>
<tr>
<td>08556001</td>
<td>An internal fan in power supply [arg1] is operating outside the recommended speed.</td>
<td>Yes</td>
</tr>
<tr>
<td>08556002</td>
<td>An internal fan in power supply [arg1] is operating outside the recommended speed.</td>
<td>Yes</td>
</tr>
<tr>
<td>08556003</td>
<td>An internal fan in power supply [arg1] is operating outside the recommended speed.</td>
<td>Yes</td>
</tr>
<tr>
<td>08556004</td>
<td>An internal fan in power supply [arg1] is operating outside the recommended speed.</td>
<td>Yes</td>
</tr>
<tr>
<td>08556005</td>
<td>An internal fan in power supply [arg1] is operating outside the recommended speed.</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Table 11. Events that automatically notify Support (continued)

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Message String</th>
<th>Automatically Notify Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>08556006</td>
<td>An internal fan in power supply [arg1] is operating outside the recommended speed.</td>
<td>Yes</td>
</tr>
<tr>
<td>0901E000</td>
<td>Chassis front LED card not present.</td>
<td>Yes</td>
</tr>
<tr>
<td>0901E003</td>
<td>Chassis rear LED card not present.</td>
<td>Yes</td>
</tr>
<tr>
<td>0E010001</td>
<td>Node [arg1] device [arg2][[arg3]] VPD is not available.</td>
<td>Yes</td>
</tr>
<tr>
<td>0E010002</td>
<td>Node [arg1] device [arg2][[arg3]] VPD is not available.</td>
<td>Yes</td>
</tr>
<tr>
<td>0E010003</td>
<td>Node [arg1] device [arg2][[arg3]] VPD is not available.</td>
<td>Yes</td>
</tr>
<tr>
<td>0E010004</td>
<td>Node [arg1] device [arg2][[arg3]] VPD is not available.</td>
<td>Yes</td>
</tr>
<tr>
<td>0E010005</td>
<td>Node [arg1] device [arg2][[arg3]] VPD is not available.</td>
<td>Yes</td>
</tr>
<tr>
<td>0E010006</td>
<td>Node [arg1] device [arg2][[arg3]] VPD is not available.</td>
<td>Yes</td>
</tr>
<tr>
<td>0E010007</td>
<td>Node [arg1] device [arg2][[arg3]] VPD is not available.</td>
<td>Yes</td>
</tr>
<tr>
<td>0E010008</td>
<td>Node [arg1] device [arg2][[arg3]] VPD is not available.</td>
<td>Yes</td>
</tr>
<tr>
<td>0E010009</td>
<td>Node [arg1] device [arg2][[arg3]] VPD is not available.</td>
<td>Yes</td>
</tr>
<tr>
<td>0E01000A</td>
<td>Node [arg1] device [arg2][[arg3]] VPD is not available.</td>
<td>Yes</td>
</tr>
<tr>
<td>0E01000B</td>
<td>Node [arg1] device [arg2][[arg3]] VPD is not available.</td>
<td>Yes</td>
</tr>
<tr>
<td>0E01000C</td>
<td>Node [arg1] device [arg2][[arg3]] VPD is not available.</td>
<td>Yes</td>
</tr>
<tr>
<td>0E01000D</td>
<td>Node [arg1] device [arg2][[arg3]] VPD is not available.</td>
<td>Yes</td>
</tr>
<tr>
<td>0E01000E</td>
<td>Node [arg1] device [arg2][[arg3]] VPD is not available.</td>
<td>Yes</td>
</tr>
<tr>
<td>0EA00001</td>
<td>I/O module [arg1] fault.</td>
<td>Yes</td>
</tr>
<tr>
<td>0EA00002</td>
<td>I/O module [arg1] fault.</td>
<td>Yes</td>
</tr>
<tr>
<td>0EA00003</td>
<td>I/O module [arg1] fault.</td>
<td>Yes</td>
</tr>
<tr>
<td>0EA00004</td>
<td>I/O module [arg1] fault.</td>
<td>Yes</td>
</tr>
<tr>
<td>0EA1A401</td>
<td>I/O module [arg1] current fault.</td>
<td>Yes</td>
</tr>
<tr>
<td>0EA1A402</td>
<td>I/O module [arg1] current fault.</td>
<td>Yes</td>
</tr>
<tr>
<td>0EA1A403</td>
<td>I/O module [arg1] current fault.</td>
<td>Yes</td>
</tr>
<tr>
<td>0EA1A404</td>
<td>I/O module [arg1] current fault.</td>
<td>Yes</td>
</tr>
<tr>
<td>0EA1F801</td>
<td>I/O module [arg1] communication failure.</td>
<td>Yes</td>
</tr>
<tr>
<td>0EA1F802</td>
<td>I/O module [arg1] communication failure.</td>
<td>Yes</td>
</tr>
<tr>
<td>0EA1F803</td>
<td>I/O module [arg1] communication failure.</td>
<td>Yes</td>
</tr>
<tr>
<td>0EA1F804</td>
<td>I/O module [arg1] communication failure.</td>
<td>Yes</td>
</tr>
<tr>
<td>0EA2D001</td>
<td>The internal proprietary management credentials for [arg1] are incorrect with error code: [arg2].</td>
<td>Yes</td>
</tr>
<tr>
<td>0EA2D002</td>
<td>The internal proprietary management credentials for [arg1] are incorrect with error code: [arg2].</td>
<td>Yes</td>
</tr>
<tr>
<td>Event ID</td>
<td>Message String</td>
<td>Automatically Notify Support</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>0EA2D003</td>
<td>The internal proprietary management credentials for [arg1] are incorrect with error code: [arg2].</td>
<td>Yes</td>
</tr>
<tr>
<td>0EA2D004</td>
<td>The internal proprietary management credentials for [arg1] are incorrect with error code: [arg2].</td>
<td>Yes</td>
</tr>
<tr>
<td>35010481</td>
<td>Node [arg1] device [arg2][arg3] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>35010482</td>
<td>Node [arg1] device [arg2][arg3] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>35010483</td>
<td>Node [arg1] device [arg2][arg3] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>35010484</td>
<td>Node [arg1] device [arg2][arg3] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>35010485</td>
<td>Node [arg1] device [arg2][arg3] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>35010486</td>
<td>Node [arg1] device [arg2][arg3] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>35010487</td>
<td>Node [arg1] device [arg2][arg3] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>35010488</td>
<td>Node [arg1] device [arg2][arg3] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>35010489</td>
<td>Node [arg1] device [arg2][arg3] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>3501048A</td>
<td>Node [arg1] device [arg2][arg3] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>3501048B</td>
<td>Node [arg1] device [arg2][arg3] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>3501048C</td>
<td>Node [arg1] device [arg2][arg3] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>3501048D</td>
<td>Node [arg1] device [arg2][arg3] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>3501048E</td>
<td>Node [arg1] device [arg2][arg3] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>35010801</td>
<td>Unexpected exception affecting [arg1] was encountered in security service.</td>
<td>Yes</td>
</tr>
<tr>
<td>35010802</td>
<td>Unexpected exception affecting [arg1] was encountered in security service.</td>
<td>Yes</td>
</tr>
<tr>
<td>35010803</td>
<td>Unexpected exception affecting [arg1] was encountered in security service.</td>
<td>Yes</td>
</tr>
<tr>
<td>35010804</td>
<td>Unexpected exception affecting [arg1] was encountered in security service.</td>
<td>Yes</td>
</tr>
<tr>
<td>35010805</td>
<td>Unexpected exception affecting [arg1] was encountered in security service.</td>
<td>Yes</td>
</tr>
<tr>
<td>35010806</td>
<td>Unexpected exception affecting [arg1] was encountered in security service.</td>
<td>Yes</td>
</tr>
<tr>
<td>35010807</td>
<td>Unexpected exception affecting [arg1] was encountered in security service.</td>
<td>Yes</td>
</tr>
<tr>
<td>35010808</td>
<td>Unexpected exception affecting [arg1] was encountered in security service.</td>
<td>Yes</td>
</tr>
<tr>
<td>35010809</td>
<td>Unexpected exception affecting [arg1] was encountered in security service.</td>
<td>Yes</td>
</tr>
<tr>
<td>3501080A</td>
<td>Unexpected exception affecting [arg1] was encountered in security service.</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Table 11. Events that automatically notify Support (continued)

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Message String</th>
<th>Automatically Notify Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>3501080B</td>
<td>Unexpected exception affecting [arg1] was encountered in security service.</td>
<td>Yes</td>
</tr>
<tr>
<td>3501080C</td>
<td>Unexpected exception affecting [arg1] was encountered in security service.</td>
<td>Yes</td>
</tr>
<tr>
<td>3501080D</td>
<td>Unexpected exception affecting [arg1] was encountered in security service.</td>
<td>Yes</td>
</tr>
<tr>
<td>3501080E</td>
<td>Unexpected exception affecting [arg1] was encountered in security service.</td>
<td>Yes</td>
</tr>
<tr>
<td>35010841</td>
<td>Unexpected exception was encountered in security service or system-management processor on [arg1].</td>
<td>Yes</td>
</tr>
<tr>
<td>35010842</td>
<td>Unexpected exception was encountered in security service or system-management processor on [arg1].</td>
<td>Yes</td>
</tr>
<tr>
<td>35010843</td>
<td>Unexpected exception was encountered in security service or system-management processor on [arg1].</td>
<td>Yes</td>
</tr>
<tr>
<td>35010844</td>
<td>Unexpected exception was encountered in security service or system-management processor on [arg1].</td>
<td>Yes</td>
</tr>
<tr>
<td>35010845</td>
<td>Unexpected exception was encountered in security service or system-management processor on [arg1].</td>
<td>Yes</td>
</tr>
<tr>
<td>35010846</td>
<td>Unexpected exception was encountered in security service or system-management processor on [arg1].</td>
<td>Yes</td>
</tr>
<tr>
<td>35010847</td>
<td>Unexpected exception was encountered in security service or system-management processor on [arg1].</td>
<td>Yes</td>
</tr>
<tr>
<td>35010848</td>
<td>Unexpected exception was encountered in security service or system-management processor on [arg1].</td>
<td>Yes</td>
</tr>
<tr>
<td>35010849</td>
<td>Unexpected exception was encountered in security service or system-management processor on [arg1].</td>
<td>Yes</td>
</tr>
<tr>
<td>3501084A</td>
<td>Unexpected exception was encountered in security service or system-management processor on [arg1].</td>
<td>Yes</td>
</tr>
<tr>
<td>3501084B</td>
<td>Unexpected exception was encountered in security service or system-management processor on [arg1].</td>
<td>Yes</td>
</tr>
<tr>
<td>3501084C</td>
<td>Unexpected exception was encountered in security service or system-management processor on [arg1].</td>
<td>Yes</td>
</tr>
<tr>
<td>3501084D</td>
<td>Unexpected exception was encountered in security service or system-management processor on [arg1].</td>
<td>Yes</td>
</tr>
<tr>
<td>3501084E</td>
<td>Unexpected exception was encountered in security service or system-management processor on [arg1].</td>
<td>Yes</td>
</tr>
<tr>
<td>35010A00</td>
<td>Chassis Management Module configuration is not compliant with the security policy.</td>
<td>Yes</td>
</tr>
<tr>
<td>4001711E</td>
<td>Standby Chassis Management Module failed to synchronize with the primary CMM. Standby network interface is disabled.</td>
<td>Yes</td>
</tr>
<tr>
<td>40040000</td>
<td>Chassis VPD is not valid.</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Table 11. Events that automatically notify Support (continued)

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Message String</th>
<th>Automatically Notify Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>40040001</td>
<td>Chassis VPD is not available.</td>
<td>Yes</td>
</tr>
<tr>
<td>40040101</td>
<td>I/O module [arg1] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>40040102</td>
<td>I/O module [arg1] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>40040103</td>
<td>I/O module [arg1] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>40040104</td>
<td>I/O module [arg1] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>40040201</td>
<td>Chassis Management Module [arg1] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>40040202</td>
<td>Chassis Management Module [arg1] VPD is not valid.</td>
<td>Yes</td>
</tr>
<tr>
<td>40040401</td>
<td>Chassis Management Module [arg1] VPD is not available.</td>
<td>Yes</td>
</tr>
<tr>
<td>40040402</td>
<td>Chassis Management Module [arg1] VPD is not available.</td>
<td>Yes</td>
</tr>
<tr>
<td>40040501</td>
<td>Chassis Management Module [arg1] is not compatible.</td>
<td>Yes</td>
</tr>
<tr>
<td>40040502</td>
<td>Chassis Management Module [arg1] is not compatible.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020000</td>
<td>Not reading device on system management (I2C) bus [arg1]. Chassis Management Module in the chassis [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020101</td>
<td>Not reading device on system management (I2C) bus [arg1]. The rear LED card in the chassis [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020102</td>
<td>Not reading device on system management (I2C) bus [arg1]. The rear LED card in the chassis [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020201</td>
<td>Not reading device on system management (I2C) bus [arg1]. Fan logic module [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020202</td>
<td>Not reading device on system management (I2C) bus [arg1]. Fan logic module [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020281</td>
<td>Not reading device on system management (I2C) bus [arg1]. Fan logic module [arg2] VPD communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020282</td>
<td>Not reading device on system management (I2C) bus [arg1]. Fan logic module [arg2] VPD communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020301</td>
<td>Not reading device on system management (I2C) bus [arg1]. I/O module [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020302</td>
<td>Not reading device on system management (I2C) bus [arg1]. I/O module [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020303</td>
<td>Not reading device on system management (I2C) bus [arg1]. I/O module [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020304</td>
<td>Not reading device on system management (I2C) bus [arg1]. I/O module [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020401</td>
<td>Not reading device on system management (I2C) bus [arg1]. Fan module [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>Event ID</td>
<td>Message String</td>
<td>Automatically Notify Support</td>
</tr>
<tr>
<td>----------</td>
<td>----------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>50020402</td>
<td>Not reading device on system management (I2C) bus [arg1]. Fan module [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020403</td>
<td>Not reading device on system management (I2C) bus [arg1]. Fan module [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020404</td>
<td>Not reading device on system management (I2C) bus [arg1]. Fan module [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020405</td>
<td>Not reading device on system management (I2C) bus [arg1]. Fan module [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020406</td>
<td>Not reading device on system management (I2C) bus [arg1]. Fan module [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020407</td>
<td>Not reading device on system management (I2C) bus [arg1]. Fan module [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020408</td>
<td>Not reading device on system management (I2C) bus [arg1]. Fan module [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020409</td>
<td>Not reading device on system management (I2C) bus [arg1]. Fan module [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>5002040A</td>
<td>Not reading device on system management (I2C) bus [arg1]. Fan module [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020501</td>
<td>Not reading device on system management (I2C) bus [arg1]. Power supply [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020502</td>
<td>Not reading device on system management (I2C) bus [arg1]. Power supply [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020503</td>
<td>Not reading device on system management (I2C) bus [arg1]. Power supply [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020504</td>
<td>Not reading device on system management (I2C) bus [arg1]. Power supply [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020505</td>
<td>Not reading device on system management (I2C) bus [arg1]. Power supply [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020506</td>
<td>Not reading device on system management (I2C) bus [arg1]. Power supply [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020601</td>
<td>Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020602</td>
<td>Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020603</td>
<td>Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020604</td>
<td>Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020605</td>
<td>Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020606</td>
<td>Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>Event ID</td>
<td>Message String</td>
<td>Automatically Notify Support</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>50020607</td>
<td>Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020608</td>
<td>Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020609</td>
<td>Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>5002060A</td>
<td>Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>5002060B</td>
<td>Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>5002060C</td>
<td>Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>5002060D</td>
<td>Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>5002060E</td>
<td>Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020701</td>
<td>Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020702</td>
<td>Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020703</td>
<td>Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020704</td>
<td>Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020705</td>
<td>Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020706</td>
<td>Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020707</td>
<td>Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020708</td>
<td>Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>50020709</td>
<td>Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>5002070A</td>
<td>Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>5002070B</td>
<td>Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>5002070C</td>
<td>Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Table 11. Events that automatically notify Support (continued)

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Message String</th>
<th>Automatically Notify Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>5002070D</td>
<td>Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
<tr>
<td>5002070E</td>
<td>Not reading device on system management (I2C) bus [arg1]. Node [arg2] communication is offline.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**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.


**Front information panel LEDs**

LEDs are displayed on the front information panel and on the rear of the Flex System Carrier-Grade 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.

<table>
<thead>
<tr>
<th>LED</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backlit Lenovo logo</td>
<td>When the Lenovo logo is lit, the chassis has power.</td>
<td>If the logo is not lit and the system has power, check for active events in the Chassis Management Module web interface.</td>
</tr>
<tr>
<td>Identify</td>
<td>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.</td>
<td>If the LED is lit, check for active events in the Chassis Management Module web interface.</td>
</tr>
</tbody>
</table>
**LED** | **Description** | **Action**
---|---|---
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 Carrier-Grade chassis.

---

**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, 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. |
<table>
<thead>
<tr>
<th>LED</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fault</td>
<td>When this yellow LED is lit, it indicates that a hardware error has occurred. Check the event logs.</td>
<td></td>
</tr>
</tbody>
</table>

**Chassis module LEDs**

Each module contains LEDs that can be used to isolate failed components.


<table>
<thead>
<tr>
<th>Module name/LED</th>
<th>Description</th>
<th>User action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Chassis management module</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fault LED</td>
<td>This yellow LED is lit when an error has occurred in the CMM. The system fault LED on the chassis will also be lit.</td>
<td>If this LED is lit, check the event log for CMM-related errors and follow the corrective actions for those events.</td>
</tr>
<tr>
<td><strong>Power supply</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DC power in LED (–48 V dc supplies only)</td>
<td>This green LED is <strong>not</strong> lit if there is a dc power problem.</td>
<td>If this LED is <strong>not</strong> lit, check the CMM event log for power-related errors and follow the corrective actions for those events.</td>
</tr>
<tr>
<td>AC power in LED (200 - 240 V ac supplies only)</td>
<td>This green LED is <strong>not</strong> lit if there is an ac power problem.</td>
<td>If this LED is <strong>not</strong> lit, check the CMM event log for power-related errors and follow the corrective actions for those events.</td>
</tr>
<tr>
<td>DC power out LED</td>
<td>The green LED is <strong>not</strong> lit if there is an dc power problem.</td>
<td>If this LED is <strong>not</strong> lit, check the CMM event log for power-related errors and follow the corrective actions for those events.</td>
</tr>
<tr>
<td>Fault LED</td>
<td>This yellow LED is lit if the power supply has failed.</td>
<td>If this LED is lit, check the CMM event log for power-related errors and follow the corrective actions for those events.</td>
</tr>
<tr>
<td><strong>Fan module</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fault LED</td>
<td>This yellow LED is lit if one of the fans in the fan module has failed. <strong>Note:</strong> If one of the fans in the fan module fails, the other fan will begin operating at full speed.</td>
<td>If this LED is lit, check the CMM event log for fan-related errors and follow the corrective actions for those events.</td>
</tr>
<tr>
<td><strong>Fan logic module</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fault LED</td>
<td>This yellow LED is lit if one of the fan logic modules fail.</td>
<td>If this LED is lit, check the CMM event log for fan-related errors and follow the corrective actions for those events.</td>
</tr>
</tbody>
</table>

**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.

**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 919 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 918.
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 921 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 919.
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 CMM or the I/O module.

**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.

**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://datacentersupport.lenovo.com](http://datacentersupport.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://datacentersupport.lenovo.com](http://datacentersupport.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 DHCP 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://datacentersupport.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://datacentersupport.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://datacentersupport.lenovo.com](http://datacentersupport.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://datacentersupport.lenovo.com](http://datacentersupport.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.

**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://datacentersupport.lenovo.com](http://datacentersupport.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://datacentersupport.lenovo.com](http://datacentersupport.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://datacentersupport.lenovo.com](http://datacentersupport.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://datacentersupport.lenovo.com](http://datacentersupport.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://datacentersupport.lenovo.com](http://datacentersupport.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://datacentersupport.lenovo.com](http://datacentersupport.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.

**Compute node connectivity problems**

This section provides information about where to find the information to solve compute node problems.


To determine which compute nodes are compatible with the Flex System Carrier-Grade chassis, see [http://www.lenovo.com/serverproven/](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://datacentersupport.lenovo.com](http://datacentersupport.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://datacentersupport.lenovo.com](http://datacentersupport.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 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 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" in the Flex System Chassis Management Module User's Guide.
4. 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.

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 log on the Chassis Management Module for any events that are related to the compute nodes, and solve them.
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" 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 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 chassis air filters for dust accumulation and replace if necessary (see “Replacing the filter media” on page 936 for more information).
3. Check the event log on the Chassis Management Module for rising temperature events and fan module events. 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.

4. Make sure that no stickers or labels have been placed on the perforated section of the compute node front panel. This is an air inlet to the node, stickers or labels will hinder airflow leading to high component temperatures.
5. If a fan zone is partially populated with compute nodes, make sure that the number of installed 80 mm fans is sufficient to cool the zone. Two or less nodes require only 2 fans, three to four nodes require 3 fans, five to seven nodes require all 4 fans (see “Installing components” on page 39 for more information).

**Single node overheating**

Use the information in this section to troubleshoot a single node that might be overheating.

**Action**

1. Check the event log on the Chassis Management Module for rising temperature events and fan module events. 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.
2. Make sure that no stickers or labels have been placed on the perforated section of the compute node front panel. This is an air inlet to the node, stickers or labels will hinder airflow leading to high component temperatures.

**CMM, I/O modules, or power supplies overheating**

Use the information in this section to troubleshoot CMM, I/O modules, or power supplies 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 chassis air filters for dust accumulation and replace if necessary (see “Replacing the filter media” on page 936 for more information).
3. Check the event log on the Chassis Management Module for rising temperature events and fan module events. 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.
4. Verify that all CMM, power supply, and I/O module bays on the rear of the chassis are populated with a either module or a filler. If a bay is left empty, hot air can recirculate leading to high component temperatures.
5. Verify that the air inlets on the front of the chassis (top and bottom of the bezel) are not obstructed. These inlets provide cool air to components in the rear of the chassis.

**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 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” 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 Power In light is not lit, make sure that the source it is connected to is powered and that the power cord is functional.
• If the Power In light remains off, replace the power supply.
• If the Power 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://datacentersupport.lenovo.com](http://datacentersupport.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://datacentersupport.lenovo.com](http://datacentersupport.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://datacentersupport.lenovo.com](http://datacentersupport.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://datacentersupport.lenovo.com](http://datacentersupport.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
1. 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.
2. Check the chassis air filters for dust accumulation and replace if necessary (see “Replacing the filter media” on page 936 for more information).
3. If all of the chassis fans are running at full speed, the chassis may not be communicating with the CMM. Check the CMM status LEDs (see “CMM controls and indicators” on page 14).

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://datacentersupport.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://datacentersupport.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, Type 7385

Use this information to locate and identify replaceable components that are available for the Flex System Carrier-Grade chassis.

For an updated parts listing go to http://datacentersupport.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 Carrier-Grade chassis.

For information about the terms of the warranty, see the Warranty Information document that comes with the Flex System Carrier-Grade chassis.
<table>
<thead>
<tr>
<th>Index</th>
<th>Description</th>
<th>CRU part number (Tier 1)</th>
<th>CRU part number (Tier 2)</th>
<th>FRU part number</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Lenovo Flex System Chassis Management Module</td>
<td>00FG678 or 01PF404</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Fan module, 40 mm</td>
<td>81Y2911</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Fan logic module</td>
<td>94Y5805</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>I/O module</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Shuttle (with card and cable assembly)</td>
<td></td>
<td></td>
<td>00MN100</td>
</tr>
<tr>
<td>10</td>
<td>LED card, rear</td>
<td></td>
<td></td>
<td>comes with midplane FRU only 00JX989</td>
</tr>
<tr>
<td>11</td>
<td>2500 W 48 V power supply, 48 to 60 V dc, 2 position power connector</td>
<td>94Y8265 or 94Y8296</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>2500 W power supply</td>
<td>00YJ931 or 00YJ910</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>2500 W power supply, 200 - 240 V ac, C20 connector</td>
<td>94Y8303, 94Y8307, 69Y5890 or 94Y8251</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>2500 W power supply,</td>
<td>00MX939 or 00MX920</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Midplane and rear LED card</td>
<td></td>
<td></td>
<td>00JX989 or 00MP727</td>
</tr>
<tr>
<td>13</td>
<td>Fan distribution card</td>
<td></td>
<td></td>
<td>81Y2980</td>
</tr>
<tr>
<td>15</td>
<td>Fan module, 80 mm</td>
<td>81Y2910</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>LED card, front</td>
<td></td>
<td></td>
<td>81Y2901</td>
</tr>
<tr>
<td></td>
<td>Battery, 3.0 V (Chassis Management Module)</td>
<td>33F8354</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Chassis cable kit, includes the following cables:</td>
<td></td>
<td></td>
<td>49Y4993</td>
</tr>
<tr>
<td></td>
<td>- Cable, rear LED card to front LED card</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Cable, 40 mm fan module to fan distribution card</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Cable, fan logic module to fan distribution card</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Console breakout cable</td>
<td>81Y5287</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Damper, node bay</td>
<td></td>
<td></td>
<td>81Y2904</td>
</tr>
<tr>
<td></td>
<td>Nameplate (includes chassis nameplate and front information panel label)</td>
<td>00MN090</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Serial cable, mini USB to RJ45 (FC9340)</td>
<td>90Y9340</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Serial cable, mini USB to DB9 (FC0510)</td>
<td>43X0510</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cable, KVM module VGA</td>
<td>00AK143</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cable, 1.5 m passive DAC SFP+</td>
<td>00AY762</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cable, 2 m passive DAC SFP+</td>
<td>00AY763</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cable, 7 m passive DAC SFP+</td>
<td>00D6150</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Index</td>
<td>Description</td>
<td>CRU part number (Tier 1)</td>
<td>CRU part number (Tier 2)</td>
<td>FRU part number</td>
</tr>
<tr>
<td>-------</td>
<td>-------------------------------------------------------</td>
<td>--------------------------</td>
<td>--------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td></td>
<td>Cable, 0.5 m passive DAC SFP+</td>
<td>00D6289</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cable, 1m Passive DAC SFP+ Cable</td>
<td>90Y9426</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cable, 3m Passive DAC SFP+ Cable</td>
<td>90Y9429</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cable, 5m Passive DAC SFP+ Cable</td>
<td>90Y9432</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cable, 1m LC-LC Fiber</td>
<td>39M5699</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cable, 5m LC-LC Fiber</td>
<td>39M5700</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cable, 25m LC-LC Fiber</td>
<td>39M5701</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cable, 0.6m blue Cat5e</td>
<td>40K8966</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cable, 1.5m blue Cat5e</td>
<td>40K8967</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cable, 3m blue Cat5e</td>
<td>40K8968</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cable, 10m blue Cat5e</td>
<td>40K8969</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cable, 25m blue Cat5e</td>
<td>40K8970</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cable, 0.6m yellow Cat5e</td>
<td>40K8971</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cable, 1.5m yellow Cat5e</td>
<td>40K8972</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cable, 3m yellow Cat5e</td>
<td>40K8973</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cable, 10m yellow Cat5e</td>
<td>40K8974</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cable, 25m yellow Cat5e</td>
<td>40K8975</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cable, 0.6m green Cat5e</td>
<td>40K8976</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cable, 1.5m green Cat5e</td>
<td>40K8977</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cable, 3m green Cat5e</td>
<td>40K8978</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cable, 10m green Cat5e</td>
<td>40K8979</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cable, 25m green Cat5e</td>
<td>40K8980</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cable, 10m black Cat5e</td>
<td>41Y9303</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Power cord, 4.3m, 16A/208 V, C19 to NEMA L6-20P (US)</td>
<td>39M5279</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Power cord, 2m, 16A/100-250 V, C19 to IEC 320-C20 Rack Power</td>
<td>39M5388</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Power cord, 2.5m, 16A/100-240 V, C19 to IEC 320-C20 Rack Power</td>
<td>39M5389</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Power cord, 4.3m, US/CAN, NEMA L15-30P - (3P+N+Gnd) to 3X IEC 320 C19</td>
<td>69Y1612</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Power cord, 4.3m, EMEA/AP, IEC 309 32A (3P+N+Gnd) to 3X IEC 320 C19</td>
<td>69Y1614</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Power cord, 4.3m, A/NZ, (PDL/Clipsal) 32A (3P+N+Gnd) to 3X IEC 320 C19</td>
<td>69Y1616</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Transceiver module, 10GBASE-SR Short range</td>
<td>46C3449</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Transceiver module, 10GbE 850 nm fiber SFP+ Ethernet</td>
<td>46C9249</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Index</td>
<td>Description</td>
<td>CRU part number (Tier 1)</td>
<td>CRU part number (Tier 2)</td>
<td>FRU part number</td>
</tr>
<tr>
<td>-------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------------------------</td>
<td>--------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>1</td>
<td>Chassis shell (without shuttle)</td>
<td>00FG027</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Filler, CMM</td>
<td>81Y2898</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Filler, power supply</td>
<td>81Y2896</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Filler, I/O module</td>
<td>81Y2897</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Filler, 80 mm fan module</td>
<td>81Y2899</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>1U filter retainer with filter</td>
<td>00MN096</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>1U bezel</td>
<td>00MN092</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Airborne contaminant filter assembly (10U filter bezel with filter retainer and mounting brackets)</td>
<td>00MN095</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dust filter replacement pack (includes four 10U filters and four 1U filters)</td>
<td>43W9057</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Chassis shelf (required for 1-bay nodes)</td>
<td>81Y2905</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Filler, node bay</td>
<td>81Y2895</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lift handle kit (includes 4 chassis lift handles)</td>
<td>81Y2902</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Miscellaneous parts kit</td>
<td>81Y2903</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Rail kit</td>
<td>88Y6721</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Support brackets (includes chassis mounting hardware)</td>
<td>00FG036</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Torx 1/4&quot; drive handle</td>
<td>9900712</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Torx bit set</td>
<td>93F2830</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. See [http://www.lenovo.com/serverproven/](http://www.lenovo.com/serverproven/) for a list of the I/O modules that are compatible with the Flex System Carrier-Grade chassis.

2. Do not mix different types of power supplies. Each chassis must contain either all dc-powered supplies or all ac-powered supplies.

**Consumable and structural parts**

Consumable and structural parts are not covered by the Statement of Limited Warranty.

<table>
<thead>
<tr>
<th>Index</th>
<th>Description</th>
<th>Part number</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Chassis shell (without shuttle)</td>
<td>00FG027</td>
</tr>
<tr>
<td>5</td>
<td>Filler, CMM</td>
<td>81Y2898</td>
</tr>
<tr>
<td>6</td>
<td>Filler, power supply</td>
<td>81Y2896</td>
</tr>
<tr>
<td>8</td>
<td>Filler, I/O module</td>
<td>81Y2897</td>
</tr>
<tr>
<td>14</td>
<td>Filler, 80 mm fan module</td>
<td>81Y2899</td>
</tr>
<tr>
<td>17</td>
<td>1U filter retainer with filter</td>
<td>00MN096</td>
</tr>
<tr>
<td>18</td>
<td>1U bezel</td>
<td>00MN092</td>
</tr>
<tr>
<td>19</td>
<td>Airborne contaminant filter assembly (10U filter bezel with filter retainer and mounting brackets)</td>
<td>00MN095</td>
</tr>
<tr>
<td></td>
<td>Dust filter replacement pack (includes four 10U filters and four 1U filters)</td>
<td>43W9057</td>
</tr>
<tr>
<td></td>
<td>Chassis shelf (required for 1-bay nodes)</td>
<td>81Y2905</td>
</tr>
<tr>
<td></td>
<td>Filler, node bay</td>
<td>81Y2895</td>
</tr>
<tr>
<td></td>
<td>Lift handle kit (includes 4 chassis lift handles)</td>
<td>81Y2902</td>
</tr>
<tr>
<td></td>
<td>Miscellaneous parts kit</td>
<td>81Y2903</td>
</tr>
<tr>
<td></td>
<td>Rail kit</td>
<td>88Y6721</td>
</tr>
<tr>
<td></td>
<td>Support brackets (includes chassis mounting hardware)</td>
<td>00FG036</td>
</tr>
<tr>
<td></td>
<td>Torx 1/4&quot; drive handle</td>
<td>9900712</td>
</tr>
<tr>
<td></td>
<td>Torx bit set</td>
<td>93F2830</td>
</tr>
</tbody>
</table>

**Power cords**

The power cords that are available for use with the Flex System Carrier-Grade chassis are determined by your country or region.
For your safety, Lenovo provides ac power cords with a grounded attachment plug to use with this product. To avoid electrical shock, always use the ac 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 table lists the -48 V dc power cord CRU part number.

**Table 12.** -48 V dc power cord

<table>
<thead>
<tr>
<th>Country</th>
<th>CRU part number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All countries</td>
<td>69Y1652</td>
<td>6-foot, 75 V dc, 120 A, two 6 AWG conductors, 5.7 mm pin flexible line cord</td>
</tr>
</tbody>
</table>

**Note:** Use the Flex System -48 V dc power cord only with -48 V dc power supply CRU number 94Y8265.

The following table lists the single-phase ac power cord CRU part number.

**Table 13.** Single-phase ac power cord

<table>
<thead>
<tr>
<th>Country</th>
<th>CRU part number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>39M5279</td>
<td>4.3m, 16A/208V, C19 to NEMA L6-20P (US) line cord</td>
</tr>
</tbody>
</table>

The following table lists the three-phase ac power cord CRU part numbers.

**Table 14.** Three-phase ac power cords

<table>
<thead>
<tr>
<th>Country</th>
<th>CRU part number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>69Y1612</td>
<td>4.3m, US/CAN, NEMA L15-30P - (3P+Gnd) to 3X IEC 320 C19 line cord</td>
</tr>
<tr>
<td>Australia/New Zealand</td>
<td>69Y1616</td>
<td>4.3m, A/NZ, (PDL/Clipsal) 32A (3P+N+Gnd) to 3X IEC 320 C19 line cord</td>
</tr>
<tr>
<td>Europe/Middle East/Africa</td>
<td>69Y1614</td>
<td>4.3m, EMEA/AP, IEC 309 32A (3P+N+Gnd) to 3X IEC 320 C19 line cord</td>
</tr>
</tbody>
</table>
Chapter 6. Removing and replacing components

Use this information to remove and replace components of the Flex System Carrier-Grade 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 Carrier-Grade 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 936. 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](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/](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
Use these instructions to remove and replace the dust filters in the airborne contaminant filter assembly and 1U filter retainer. You can replace the dust filters while the chassis is powered on.

The airborne contaminant filters are a consumable part. It is not covered under the terms of the warranty. Use Table 15 “Suggested inspection and replacement intervals” on page 936 as a guide to help you determine when to replace the filter media in the filter assembly.

<table>
<thead>
<tr>
<th>Environment</th>
<th>Visually inspect and clean</th>
<th>Replace filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low dust, low foot traffic</td>
<td>3 months</td>
<td>6 months</td>
</tr>
<tr>
<td>Moderate dust, moderate foot traffic</td>
<td>6 weeks</td>
<td>3 months</td>
</tr>
<tr>
<td>Heavy dust, heavy foot traffic</td>
<td>2 weeks</td>
<td>1 month</td>
</tr>
</tbody>
</table>

Table 15. *Suggested inspection and replacement intervals*
**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" in the *Lenovo Flex System Chassis Management Module User’s Guide* for more information.

Both the 10U and 1U filters are made of a premium quality flame-retardant reticulated filter foam. The filters meet the Underwriters Laboratories Inc. flame class of UL94 HF-1 (UL file number E93229). This filter foam also meets the European RoHS standard.

### Table 16. Filter media specifications

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Color</td>
<td>Black</td>
</tr>
<tr>
<td>Base material</td>
<td>Polyether, polyester blend</td>
</tr>
<tr>
<td>Density (approximate)</td>
<td>2 - 3.2 lbs/ft³</td>
</tr>
<tr>
<td>Tensile strength, minimum</td>
<td>22 psi</td>
</tr>
<tr>
<td>Tear strength, minimum</td>
<td>4.5 lbs/inch</td>
</tr>
<tr>
<td>Elongation, minimum % to break</td>
<td>200</td>
</tr>
<tr>
<td>Cell count</td>
<td>10 - 100 ppi</td>
</tr>
<tr>
<td>Reticulation</td>
<td>Thermal (zapped)</td>
</tr>
<tr>
<td>Thickness range</td>
<td>0.15 - 1.0 inches</td>
</tr>
<tr>
<td>Flammability rating</td>
<td>UL94, HF-1</td>
</tr>
<tr>
<td>Temperature range</td>
<td>-40°F to +284°F</td>
</tr>
<tr>
<td>Dust filter replacement pack</td>
<td>43W9057 (includes four 10U filters and four 1U filters)</td>
</tr>
</tbody>
</table>

**Attention:** Do not clean and reuse the dust filters. You must discard contaminated filters and replace with new filters.

Complete the following steps to replace the airborne contaminant filter media:

**Step 1.** Replace the 10U dust filter in the airborne contaminant filter assembly.
   a. Remove the airborne contaminant filter assembly bezel from the chassis (see “Removing the airborne contaminant filter assembly” on page 961).
      
      **Note:** Remove the filter assembly bezel only. Do not remove the filter assembly mounting brackets.
   b. Push down on the slide latches on both sides of the filter assembly.
   c. Rotate the filter assembly down and remove the hooks from the slots.
   d. Turn the blue filter retainer clips to the open position and remove the filter retainer and filter.
e. Discard the old 10U filter and place a new filter on the filter assembly.

f. Place the bottom of the filter retainer behind the alignment features on the bottom of the filter bezel.

g. 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.
h. Install the airborne contaminant filter assembly bezel on the chassis (see “Replacing the airborne contaminant filter assembly” on page 962).

Step 2. Replace the 1U dust filter located behind the 1U bezel.
   a. Remove the 1U bezel from the chassis (see “Removing the 1U bezel” on page 964).
   b. Remove the 1U filter retainer from the chassis (see “Removing the 1U filter retainer” on page 965).
   c. Pull the dust filter out of the 1U filter retainer and discard it.
   d. Place the 1U filter retainer on a flat surface with the extensions up. Place a new filter over the retainer extensions and slide it down into the retainer. Bend the filter slightly and tuck the filter edges under the tabs on the filter retainer; then, press the filter edges all the way into the retainer.
   e. Install the 1U filter retainer in the chassis (see “Replacing the 1U filter retainer” on page 965).
   f. Install the 1U bezel on the chassis (see “Replacing the 1U bezel” on page 964).

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 Carrier-Grade 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 Carrier-Grade 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 "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 Carrier-Grade 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 “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 14 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,” 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 "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," in the Lenovo Flex System Chassis Management Module Installation Guide, for information.

Removing compute nodes

Use the instructions to remove compute nodes from the Flex System Carrier-Grade 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 Carrier-Grade 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. Remove the airborne contaminant filter assembly bezel (see “Removing the airborne contaminant filter assembly” on page 961).

   Note: Remove only the airborne contaminant filter assembly bezel. You do not need to remove the filter assembly mounting brackets in order to remove a compute node.

2. 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.

3. 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.

If you are not immediately replacing the compute node, install a node bay filler in the empty bay and reinstall the airborne contaminant filter assembly bezel (see “Replacing the airborne contaminant filter assembly” on page 962).

Removing a 2-bay compute node
Use these instructions to remove a 2-bay compute node from the Flex System Carrier-Grade 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. Remove the airborne contaminant filter assembly bezel (see “Removing the airborne contaminant filter assembly” on page 961).

   Note: Remove only the airborne contaminant filter assembly bezel. You do not need to remove the filter assembly mounting brackets in order to remove a compute node.

2. 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.

3. 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.

If you are not immediately replacing the compute node, complete the following steps:
1. Install a chassis shelf in the empty node bays (see “Replacing a chassis shelf” on page 960).
2. Install a node bay filler in each empty bay.
3. Reinstall the airborne contaminant filter assembly bezel (see “Replacing the airborne contaminant filter assembly” on page 962).

Replacing compute nodes

Use the instructions to replace compute nodes in the Flex System Carrier-Grade 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 Carrier-Grade 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.

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 39.

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

Step 1. Remove the airborne contaminant filter assembly bezel, if one is installed (see “Removing the airborne contaminant filter assembly” on page 961).
**Note:** Remove only the airborne contaminant filter assembly bezel. You do not need to remove the filter assembly mounting brackets in order to install a compute node.

Step 2. 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 3. Open the release handle (rotate the handle to the left).

Step 4. Slide the compute node into the node bay until it is seated.

Step 5. Close the release handle (rotate the handle to the right).

After you install the compute node, complete the following steps:

1. Make a note of the compute node identification information on one of the labels that come with the Flex System Carrier-Grade chassis. Place a label on the node label tab. See “User labels” on page 54 for more information.

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

2. Replace the airborne contaminant filter assembly bezel (see “Replacing the airborne contaminant filter assembly” on page 962).

**Replacing a 2-bay compute node**

Use these instructions to install a 2-bay compute node in the Flex System Carrier-Grade 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/](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 39.
To install a 2-bay compute node, complete the following steps:

Step 1. Remove the airborne contaminant filter assembly bezel, if one is installed (see “Removing the airborne contaminant filter assembly” on page 961).

   **Note:** Remove only the airborne contaminant filter assembly bezel. You do not need to remove the filter assembly mounting brackets in order to install a compute node.

Step 2. Remove the node bay fillers, if they are installed. Push the filler release tab to the right; then, grasp the filler by the slot and pull it out of the bay.

Step 3. Remove the chassis shelf, if one is installed (see “Removing a chassis shelf” on page 960).

Step 4. Open both release handles (rotate the left handle to the left and rotate the right handle to the right).

Step 5. Slide the compute node into the node bays until it is seated.

Step 6. Close both release handles.

After you install the compute node, complete the following steps:

1. Make a note of the compute node identification information on the labels that come with the Flex System Carrier-Grade chassis. Place a label on the node label tab. See “User labels” on page 54 for more information.

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

2. Replace the airborne contaminant filter assembly bezel (see “Replacing the airborne contaminant filter assembly” on page 962).

**Removing fan modules**

Use the instructions to remove fan modules from the Flex System Carrier-Grade chassis, depending on the type of fan module.

**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 5 minutes to maintain adequate cooling.
Do not operate the chassis without a 80 mm fan module or a 80 mm filler in each 80 mm fan bay. When you remove a 80 mm fan module in a typical environment, install a new 80 mm fan within 2 minutes to maintain adequate cooling. In an extreme environment, you must install a new 80 mm fan within 30 seconds to maintain adequate cooling.

Both the 40 mm and 80 mm fans can be hot swapped. It requires an estimated 15 seconds to remove and replace a fan module.

Removing a 40 mm fan module
Use these instructions to remove a 40 mm fan module from the Flex System Carrier-Grade 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 5 minutes 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 Carrier-Grade chassis.

Attention: Do not operate the chassis without a 80 mm fan module or a 80 mm filler in each 80 mm fan bay. When you remove a 80 mm fan module in a typical environment, install a new 80 mm fan within 2 minutes to maintain adequate cooling. In an extreme environment, you must install a new 80 mm fan within 30 seconds to maintain adequate cooling.

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 Carrier-Grade chassis, depending on the type of fan module.

**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 5 minutes to maintain adequate cooling.
- Do not operate the chassis without a 80 mm fan module or a 80 mm filler in each 80 mm fan bay. When you remove a 80 mm fan module in a typical environment, install a new 80 mm fan within 2 minutes to maintain adequate cooling. In an extreme environment, you must install a new 80 mm fan within 30 seconds to maintain adequate cooling.
- Both the 40 mm and 80 mm fans can be hot swapped. It requires an estimated 15 seconds to remove and replace a fan module.

**Replacing a 40 mm fan module**

Use these instructions to install a 40 mm fan module in the Flex System Carrier-Grade 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 Carrier-Grade chassis. You can install a 80 mm fan module while the Flex System Carrier-Grade chassis is powered on.

See “Installing components” on page 39 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 Carrier-Grade chassis.

Before you remove the I/O module, complete the following steps:

1. If possible, power down the I/O module 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.

![I/O module diagram]

**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 Carrier-Grade chassis. You can install an I/O module while the Flex System Carrier-Grade 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:

2. Verify that the I/O module is compatible with the chassis. See [http://www.lenovo.com/serverproven/](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.

**Warning:** The intra-building port(s) (EN2092 I/O module Ethernet ports) of the equipment or subassembly are suitable for connection to intra-building or unexposed wiring or cabling only. The intra-building port(s) of the equipment or subassembly MUST NOT be metallically connected to interfaces that connect to the OSP or its wiring. These interfaces are designed for use as intra-building interfaces only (Type 2 or Type 4 ports as described in GR-1089) and require isolation from the exposed OSP cabling. The addition of Primary Protectors is not sufficient protection in order to connect these interfaces metallically to OSP wiring.

**Attention:** All CAT-5E cables used for the Flex System Carrier-Grade chassis must be shielded and grounded on both ends.

**Removing a power supply**

Use these instructions to remove a power supply from the Flex System Carrier-Grade 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.

<table>
<thead>
<tr>
<th>To Connect:</th>
<th>To Disconnect:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Turn OFF all power sources and equipment that is to be attached to this product.</td>
<td>1. Turn OFF all power sources and equipment that is to be attached to this product.</td>
</tr>
<tr>
<td>2. Attach signal cables to the product.</td>
<td>• For ac systems, remove all power cords from the chassis power receptacles or interrupt power at the ac power distribution unit.</td>
</tr>
<tr>
<td>3. Attach power cords to the product.</td>
<td>• For dc systems, disconnect dc power sources at the breaker panel or by turning off the power source. Then, remove the dc cables.</td>
</tr>
<tr>
<td>• For ac systems, use appliance inlets.</td>
<td>2. Remove the signal cables from the connectors.</td>
</tr>
<tr>
<td>• 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.</td>
<td>3. Remove all cables from the devices.</td>
</tr>
<tr>
<td>4. Attach signal cables to other devices.</td>
<td></td>
</tr>
<tr>
<td>5. Connect power cords to their sources.</td>
<td></td>
</tr>
<tr>
<td>6. Turn ON all the power sources.</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Breaker</th>
<th>Ground cable</th>
<th>Torque rating for ground screws</th>
</tr>
</thead>
<tbody>
<tr>
<td>Listed 70 A</td>
<td>4 AWG with Listed lug which can accept M6 ground screws</td>
<td>4.0 - 4.8 Newton-meters (35.4 - 42.5 inch-pounds)</td>
</tr>
</tbody>
</table>

1. The maximum steady state current of the -48 V dc power supply is less than 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 Carrier-Grade chassis without a power supply or power-supply filler in each power supply bay. Install a power supply or filler within 1 minute of the removal of a power supply.

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 Carrier-Grade chassis. You can install a power supply while the Flex System Carrier-Grade 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:

<table>
<thead>
<tr>
<th>Breaker</th>
<th>Listed 70 A</th>
<th>See Note 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ground cable</td>
<td>4 AWG with Listed lug which can accept M6 ground screws</td>
<td>See Note 2</td>
</tr>
<tr>
<td>Torque rating for ground screws</td>
<td>4.0 - 4.8 Newton-meters (35.4 - 42.5 inch-pounds)</td>
<td>-</td>
</tr>
</tbody>
</table>

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:

- Do not mix different types of power supplies in the Flex System Carrier-Grade chassis.
- Each chassis must contain either all dc-powered supplies or all ac-powered supplies.
- 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 Carrier-Grade 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 Carrier-Grade 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 Carrier-Grade chassis.

Before you remove a chassis shelf, complete the following steps:

1. Read “Safety” on page iii and “Installation guidelines” on page 935
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. 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 Carrier-Grade 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 the airborne contaminant filter assembly**

Use these instructions to remove the airborne contaminant filter assembly from the Flex System Carrier-Grade chassis.

**Attention:** The captive screws that secure the airborne contaminant filter assembly mounting brackets also secure the chassis to the rack. Do not leave the chassis unsecured.

To remove the airborne contaminant filter assembly from the chassis, complete the following steps:

Step 1. Remove the airborne contaminant filter assembly bezel from the front of the chassis.
a. Push down on the slide latches on both sides of the chassis airborne contaminant filter assembly.

b. Rotate the airborne contaminant filter assembly down and remove the hooks from the slots on the chassis.

Step 2. If necessary, remove the filter assembly mounting brackets.

Replacing the airborne contaminant filter assembly

Use these instructions to replace the airborne contaminant filter assembly on the Flex System Carrier-Grade chassis.

Attention: The captive screws that secure the airborne contaminant filter assembly mounting brackets also secure the chassis to the rack. Do not leave the chassis unsecured.
To install the airborne contaminant filter assembly on the chassis, complete the following steps:

Step 1. Install the airborne contaminant filter mounting brackets on the front of the chassis:

a. Align the left mounting bracket captive screws with the four empty screw holes on the left side of the chassis bezel. Thread the four captive screws through the bezel into the clip nuts to secure the left bracket to the chassis, but do not tighten the screws.

b. Align the right mounting bracket captive screws with the four empty screw holes on the right side of the chassis bezel. Thread the four captive screws through the bezel into the clip nuts to secure the right bracket to the chassis, but do not tighten the screws.

c. After all of the captive screws are installed, tighten the screws to 30 in-lbs (3.4 Nm) to secure the chassis to the rack.

Step 2. Install the airborne contaminate filter assembly bezel on the mounting brackets:

a. Insert the two hooks on the bottom of the filter assembly into the slots on the bottom of the chassis bezel.
b. Rotate the filter assembly toward the chassis by pushing on the front of the filter assembly until the slide latches click into place. Check the hooks on the bottom of the filter assembly to make sure that they are still in the slots on the bottom of the chassis.

**Removing the 1U bezel**

Use these instructions to remove the 1U bezel from the Flex System Carrier-Grade chassis.

To remove the 1U bezel from the chassis, complete the following steps:

Step 1. Grasp the ends of the 1U bezel.

Step 2. Pull the bezel straight towards you to remove it from the chassis.

**Replacing the 1U bezel**

Use these instructions to replace the 1U bezel on the Flex System Carrier-Grade chassis.

To install the 1U bezel on the chassis, complete the following step:

Step 1. Grasp the ends of the 1U bezel; then, align the opening on the back of the bezel with the air duct on the front of the chassis.
Step 2. Slide the bezel into the air duct until it snaps into place.

**Removing the 1U filter retainer**

Use these instructions to remove the 1U filter retainer from the Flex System Carrier-Grade chassis.

To remove the 1U filter retainer from the chassis, complete the following steps:

Step 1. Remove the 1U bezel from the chassis (see “Removing the 1U bezel” on page 964).

Step 2. Grasp the extensions on the 1U filter retainer and pull it straight out of the chassis air duct.

**Important:** Do not operate the chassis for an extended period without the 1U filter. If you are replacing the 1U dust filter, see “Replacing the filter media” on page 936 for instructions.

**Replacing the 1U filter retainer**

Use these instructions to install the 1U filter retainer in the Flex System Carrier-Grade chassis.
To install the 1U filter retainer in the chassis, complete the following steps:

Step 1. Grasp the 1U filter retainer by the extensions and slide the filter retainer all the way into the chassis air duct.

Step 2. Install the 1U bezel (see “Replacing the 1U bezel” on page 964).

---

**Removing and replacing FRUs**

Field-replaceable units (FRUs) must be removed and replaced only by trained service technicians.

**Removing the shuttle**

(Trained service technician only) Use these instructions to remove the chassis shuttle from the Flex System Carrier-Grade 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 935.
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. Disconnect the chassis from power (see “Disconnecting the chassis from power” on page 55).
4. Disconnect all cables from the modules in the rear of the chassis.
5. 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 950).
   - CMM (see “Removing a Chassis Management Module” on page 939).
   - Fan modules (see “Removing a 40 mm fan module” on page 947 and “Removing a 80 mm fan module” on page 947).
   - Power supplies (see “Removing a power supply” on page 951).

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 Carrier-Grade 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 steps a through d until the screws are tightened to 1.6 Newton-meters (1.18 foot-pounds).
Attention: The four shuttle screws secure the shuttle tightly against the rear of the midplane. If these screws are not tightened to the correct torque, the shuttle might not be fully seated against 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 Carrier-Grade chassis:
   - I/O modules (see “Replacing an I/O module” on page 950).
   - CMM (see “Replacing a Chassis Management Module” on page 940).
   - Fan modules (see “Replacing a 40 mm fan module” on page 948 and “Replacing a 80 mm fan module” on page 949).
   - Power supplies (see “Replacing a power supply” on page 954).
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 50).
4. Restart any compute nodes that you shut down. See the documentation that comes with each compute node for detailed instructions.

Removing a fan distribution card

(Trained service technician only) Use these instructions to remove a fan distribution card from the Flex System Carrier-Grade chassis.

Before you remove a fan distribution card, complete the following steps:

1. Read “Safety” on page iii and “Installation guidelines” on page 935
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. Disconnect the chassis from power (see “Disconnecting the chassis from power” on page 55).
4. Disconnect all cables from the modules in the rear of the chassis.
5. Remove the components from the rear of the chassis.
6. Remove the shuttle from the chassis (see “Removing the shuttle” on page 966).

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 Carrier-Grade 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 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 968).
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 50).
5. Restart any compute nodes that you shut down. See the documentation that comes with each compute node for detailed instructions.
Removing the front LED card

Use these instructions to remove the front LED card from the Flex System Carrier-Grade 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. Disconnect the chassis from power (see “Disconnecting the chassis from power” on page 55).

**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 942 or “Removing a 2-bay compute node” on page 943).

**Step 2.** Remove the four chassis shelves from the bottom of the chassis (see “Removing a chassis shelf” on page 960 for instructions).

**Step 3.** Remove the two T-8 Torx screws that secure the card to the chassis, using a Torx driver.

**Step 4.** Slide the front panel LED card access cover back and to the right and disconnect the cable from the card.

**Step 5.** 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 Carrier-Grade 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 960).

Step 6. Reinstall the compute nodes (see “Replacing a 1-bay compute node” on page 944 or “Replacing a 2-bay compute node” on page 945).

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.

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.
Removing the midplane

(Trained service technician only) Use these instructions to remove the midplane from the Flex System Carrier-Grade chassis.

Before you remove the midplane, complete the following steps:

1. Read “Safety” on page iii and “Installation guidelines” on page 935
2. Record the machine type model, 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. Contact Support and request the UUID for the chassis serial number and the machine type model.
      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. Open the release handles on the compute nodes to disengage the nodes from the midplane connectors.
6. Disconnect the chassis from power (see “Disconnecting the chassis from power” on page 55).
7. Disconnect all cables from the modules in the rear of the chassis.
8. Remove all of the components and component bay fillers from the rear of the chassis. See the following tasks for additional instructions:
   - “Removing a power supply” on page 951
   - “Removing an I/O module” on page 950
   - “Removing a Chassis Management Module” on page 939
   - “Removing a 40 mm fan module” on page 947
   - “Removing a 80 mm fan module” on page 947
   - “Removing a fan logic module” on page 958
9. Remove the shuttle from the chassis (see “Removing the shuttle” on page 966).
10. Remove the rear LED card from the midplane (see “Removing the rear LED card” on page 977).

To remove the midplane, complete the following steps.
Step 1. Disengage the compute nodes 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 Carrier-Grade 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 978 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 968).
2. Reinstall all of the components and component bay fillers that you removed from the rear of the chassis. See the following tasks for additional instructions:
   - “Replacing a power supply” on page 954
   - “Replacing a fan logic module” on page 959
   - “Replacing a 80 mm fan module” on page 949
   - “Replacing a 40 mm fan module” on page 948
   - “Replacing a Chassis Management Module” on page 940
   - Reinstall the I/O modules in the I/O bays but do not close the I/O module release handles. See “Replacing an I/O module” on page 950.
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 50).
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](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)
mt | 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 I/O modules 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. 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 935

2. Record the machine type model, 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. Contact Support and request the UUID for the chassis serial number and the machine type model.
      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](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. Open the release handles on the compute nodes to disengage the nodes from the midplane connectors.

6. Disconnect the chassis from power (see “Disconnecting the chassis from power” on page 55).

7. Disconnect all cables from the modules in the rear of the chassis.

8. Remove all of the components and component bay fillers from the rear of the chassis. See the following tasks for additional instructions:
   - “Removing a power supply” on page 951
9. Remove the shuttle from the chassis (see “Removing the shuttle” on page 966).

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 968).
2. Reinstall all of the components and component bay fillers that you removed from the rear of the chassis. See the following tasks for additional instructions:
   - “Replacing a power supply” on page 954
   - “Replacing a fan logic module” on page 959
   - “Replacing a 80 mm fan module” on page 949
   - “Replacing a 40 mm fan module” on page 948
   - “Replacing a Chassis Management Module” on page 940
   - Reinstall the I/O modules in the I/O bays but do not close the I/O module release handles. See “Replacing an I/O module” on page 950.
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 50).
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:

<table>
<thead>
<tr>
<th>vpdrep command arguments</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-sn</td>
<td>Chassis serial number (7 alphanumeric characters)</td>
</tr>
<tr>
<td>-tm</td>
<td>Machine type model (7 alphanumeric characters)</td>
</tr>
<tr>
<td>-uuid</td>
<td>Universally unique identifier (32 hex digits, spaces not allowed)</td>
</tr>
</tbody>
</table>

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 I/O modules 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. The I/O Modules are powered-on automatically by the CMM.
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://datacentersupport.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://datacentersupport.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://datacentersupport.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.

愛製商/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：台北市內湖區瑞興大樓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.

© Copyright Lenovo 2015, 2019
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.
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

<table>
<thead>
<tr>
<th>Contaminant</th>
<th>Limits</th>
</tr>
</thead>
</table>
| 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 |

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.

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**

Attention: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

**European Union EMC Directive conformance statement**

This product is in conformity with the protection requirements of EU Council Directive 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

**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


Deutschland:


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."


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

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.

JEITA harmonics guideline - Japanese Statement for AC power consumption (W)

JEITA harmonics guideline - Japanese Statement of Compliance for Products Less than or Equal to 20A per phase

JEITA harmonics guideline - Japanese Statement of Compliance for Products More than 20A

Korea Communications Commission (KCC) statement

This is electromagnetic wave compatibility equipment for business (Type A). Sellers and users need to pay attention to it. This is for any areas other than home.
Russia Electromagnetic Interference (EMI) Class A statement

ВНИМАНИЕ!
Настоящее изделие относится к оборудованию класса A. 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，在生活环境使用时，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

<table>
<thead>
<tr>
<th>單元</th>
<th>Unit</th>
<th>鉛Lead (Pb)</th>
<th>汞Mercury (Hg)</th>
<th>鈮Cadmium (Cd)</th>
<th>六價鉻Hexavalent chromium (Cr⁶⁺)</th>
<th>多溴聯苯Polybrominated biphenyls (PBB)</th>
<th>多溴二苯醚Polybrominated diphenyl ethers (PBDE)</th>
</tr>
</thead>
<tbody>
<tr>
<td>機架</td>
<td>-</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>外部蓋板</td>
<td>-</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>機械組合件</td>
<td>-</td>
<td>-</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>空氣傳動設備</td>
<td>-</td>
<td>-</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>冷卻組合件</td>
<td>-</td>
<td>-</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>內存模塊</td>
<td>-</td>
<td>-</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>處理器模塊</td>
<td>-</td>
<td>-</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>電纜組合件</td>
<td>-</td>
<td>-</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>電源</td>
<td>-</td>
<td>-</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>儲備設備</td>
<td>-</td>
<td>-</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>電路卡</td>
<td>-</td>
<td>-</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>光碟機</td>
<td>-</td>
<td>-</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>雷射器</td>
<td>-</td>
<td>-</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>

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 0.1 wt%" 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

10U dust filter
replacing 936
1U bezel
removing 964
replacing 964
1U dust filter
replacing 936
1U filter retainer
removing 965
replacing 965

A
address
IPV6 initial connection 60
link local 60
airborne contaminant filter
removing 961
replacing 962
Airborne contaminant filter
replacing 936
alerts
Lenovo XClarity Administrator 915
assistance, getting 981
Australia Class A statement 988

B
bezel, 1U
removing 964
replacing 964
Brocade documentation 5

C
cabling
the chassis 50
Canada Class A electronic emission statement 988
Cannot communicate with the CMM 918
Cannot communicate with the I/O module 918
Cannot log in to the CMM 918
Cannot log in to the I/O module 919
Cannot log in, troubleshooting 918
Cannot ping the CMM, troubleshooting 919
Cannot ping the I/O module, troubleshooting 921
chassis
installing 968
China Class A electronic emission statement 991
Class A electronic emission notice 988
Clicking or rattling noises - fan module 928
Clicking or rattling noises - power supply 928
CMM
configuring the chassis 59
Ethernet connection 62
installing 940
removing 939
CMM cannot ping the CMM 920
CMM connection information 59
CMM error codes 68
CMM overheating 926
component
returning 936
components 10
Chassis Management Module 13
Compute nodes 12
fan logic modules 21
fan module 19
installing 39
I/O modules 16
power supply 17
Components
removing 24
compute node - configuring 65
firmware 55
installing 944–945
removing 942–943
troubleshooting 922
Compute node will not power off 925
compute node, 1-bay
initially installing 40
calculate node, 2-bay
initially installing 41
calculate nodes
removing 942
replacing 944
configuring 59
compute nodes 65
I/O modules 63
Configuring the chassis by using the CMM 59
Configuring the chassis by using the Lenovo XClarity Administrator 63
connecting
power to the chassis 50
connection information
CMM 59
Connectivity loss, multiple nodes 923–924
Connectivity loss, multiple nodes during initial setup 923
connectors, hot-pluggable 1
Consumable parts
removing 936
replacing 936
contamination, particulate and gaseous 987
Controls and indicators
compute node 12
cooling 7
cords, power 932
creating a personalized support web page 982
CRU 935, 939
custom support web page 982
customer replaceable unit (CRU) 935, 939

© Copyright Lenovo 2015, 2019
D
device drivers 55
device, returning 936
diagnostic tools 67
documentation CD 6
    using 982
documentation CD 6
documentation, Brocade 5
documentation, related 4
DSA, sending data 982

E
electrical input 7
electronic emission Class A notice 988
environment 7
error codes
    chassis management module 68
    CMM 68
    error LEDs 917
    Chassis Management Module 917
    fan logic modules 917
    fan module 917
    power supply 917
Ethernet connection
    CMM 62
European Union EMC Directive conformance statement 988
event log
    Lenovo XClarity Administrator 915
    event log, CMM 68
expansion capabilities 1

F
fan distribution card
    installing 970
    removing 969
fan logic module
    installing 959
    removing 958
fan logic modules
    overview 21
    fan module
        error LED 917
        overview 19
    fan module, 40 mm
        installing 948
        removing 947
    fan module, 80 mm
        initially installing 46
        installing 949
        removing 947
fan modules
    removing 946
    replacing 948
FCC Class A notice 988
features 1, 7
field replaceable unit (FRU) 935, 966
filter assembly
    removing 961
    replacing 962
Filter media
    replacing 936
firmware 55
Flex System Carrier-Grade chassis
    10, 59
    connectors, hot-pluggable 1
    expansion capabilities 1
    features 1
    hot-pluggable connectors 1
    overview 1

G
gaseous contamination 987
Germany Class A statement 989
grounding
    the chassis 48
    guidelines
        installation 935
        system reliability 935

H
hardware service and support telephone numbers 983
hardware setup 24
heat output 7
help
    from the World Wide Web 982
    from World Wide Web 982
    sending diagnostic data 982
    sources of 981
    hot-pluggable connectors 1

I
important notices 986
indicators and controls
    Chassis Management Module 14
    fan 19, 21
    power supply 17
    information center 982
    Initial setup, multiple nodes cannot connect 923
input output connectors
    Chassis Management Module 15
    installation guidelines 935
    installing
        a 40 mm fan module 948
        a 80 mm fan module 949
        a fan logic module 959
        cabling 50
        Chassis Management Module 42
        chassis shelf 960
        chassis shuttle 968
        CMM 940
        components 39
        compute node 944–945
        compute node, 1-bay 40
        compute node, 2-bay 41
        fan distribution card 970
        fan pack, 80 mm 46
        Front Panel LEDs 979
        Flex System Carrier-Grade chassis 23
        front LED card 973
        grounding 48
        I/O module 47, 950
        LED card, front 973
        midplane 975
        power supply 43, 954
        rear LED card 978
shuttle 968
installing the chassis 29
in a rack 968
I/O module 16
bays 16
configuring 63
firmware 55
initially installing 47
installing 950
overview 16
removing 950
I/O module overheating 926
Installing hardware setup 24
Intermittent connectivity problems, troubleshooting 922
IP address 62

J
Japanese electromagnetic compatibility statements 990
Jet or fast-moving air noises - fan module 928
Jet or fast-moving air noises - power supply 928

K
Korea Class A electronic emission statement 990

L
Labels, user 54
LED card, front 12
removing 972
replacing 973
LED card, rear 977
LEDs 915
chassis front information panel 12
Chassis Management Module 14
chassis rear 12, 915
compute node 12
fan 19, 21
front information panel 12, 915
overview 917
power supply 17
LEDs, chassis rear 12
Lenovo XClarity Administrator 915
configuring the chassis 63
Lenovo XClarity Administrator alerts 915
Lenovo XClarity Administrator event log 915
link local address 60

M
messages 68
chassis management module 68
IMM 68
midplane 915
installing 975
removing 974
Multiple machines overheating 925
Multiple nodes cannot connect during initial setup 923
Multiple nodes cannot connect, troubleshooting 923
Multiple nodes cannot ping the CMM 920
Multiple nodes cannot ping the I/O module 922
Multiple nodes will not power on 924
Multiple-node connectivity loss 923

N
network access tag 59
New Zealand Class A statement 988
Node power problems, troubleshooting 924
notes, important 986
notices 985
electronic emission 988
FCC, Class A 988
notices, types of 7

O
overheating, CMM, I/O modules, or power supplies 926
Overheating, troubleshooting 925
overview 12

P
part numbers 932
power cords 932
particulate contamination 987
parts listing 929
People’s Republic of China Class A electronic emission statement 991
Poor network performance, troubleshooting 926
power connecting Flex System Carrier-Grade chassis to 50
cords 932
disconnecting the chassis from 55
power supply 926
error LEDs 917
initially installing 43
installing 954
overview 17
removing 951
power supply overheating 926
Power supply problems 926
product service, Taiwan 983
publications, Brocade 5
publications, related 4

R
rack 29
installing Flex System Carrier-Grade chassis 29
rack template 37
rear chassis fault LEDs 915
rear LED card 915
installing 978
removing 977
rear view 915
Flex System Carrier-Grade chassis 12
related documentation 4
S

safety iii
safety statements iii–iv
sending diagnostic data 982
serial pinout
Chassis Management Module 15
service and support
before you call 981
hardware 983
software 982
service bulletins 67
shelf, chassis
installing 960
shelves, chassis
removing 960
shuttle
installing 968
removing 966
Single node cannot ping the CMM 919
Single node cannot ping the I/O module 921, 927
Single node overheating 925
Single node will not power on 924
Single-node connectivity loss 922
size 7
software service and support telephone numbers 982
Squealing, scratching, grinding, or groaning noises - fan module 927
Squealing, scratching, grinding, or groaning noises - power supply 927
static electricity 936
static-sensitive devices, handling 936
subnet 62
Sudden connectivity loss, multiple nodes 924
support web page, custom 982
symptoms
troubleshooting 917
system reliability guidelines 935
system specifications 7

T

Taiwan BSMI RoHS declaration 992
Taiwan Class A electronic emission statement 991
Taiwan product service 983
telecommunication regulatory statement 987
telephone numbers 935
the chassis 67
Tier 1 CRU 939
Tier 2 CRU 939

timeout 62
trademarks 986
troubleshooting 67
by symptom 917
custom compute nodes 922
service bulletins 67
Troubleshooting, cannot communicate with the CMM 918
Troubleshooting, cannot communicate with the I/O module 918
Troubleshooting, cannot log in 918
Troubleshooting, cannot log in to the CMM 918
Troubleshooting, cannot log in to the I/O module 919
Troubleshooting, cannot ping the CMM 919
Troubleshooting, cannot ping the I/O module 921
Troubleshooting, clicking or rattling noises - fan module 928
Troubleshooting, clicking or rattling noises - power supply 928
Troubleshooting, CMM cannot ping the CMM 920
Troubleshooting, CMM, I/O modules, or power supplies overheating 926
Troubleshooting, compute node will not power off 925
Troubleshooting, intermittent connectivity problems 922
Troubleshooting, jet or fast-moving air noises - fan module 928
Troubleshooting, jet or fast-moving air noises - power supply 928
Troubleshooting, multiple machines overheating 925
Troubleshooting, multiple nodes cannot connect 923
Troubleshooting, multiple nodes cannot connect during initial setup 923
Troubleshooting, multiple nodes cannot ping the CMM 920
Troubleshooting, multiple nodes cannot ping the I/O module 922
Troubleshooting, multiple nodes will not power on 924
Troubleshooting, multiple-node connectivity loss 923
Troubleshooting, node power problems 924
Troubleshooting, overheating 925
Troubleshooting, poor network performance 926
Troubleshooting, power supply problems 926
Troubleshooting, single node cannot ping the CMM 919
Troubleshooting, single node cannot ping the I/O module 921, 927
Troubleshooting, single node overheating 925
Troubleshooting, single node will not power on 924
Troubleshooting, single-node connectivity loss 922
Troubleshooting, squealing, scratching, grinding, or groaning noises - fan module 927
Troubleshooting, squealing, scratching, grinding, or groaning noises - power supply 927
Troubleshooting, sudden connectivity loss 924
Troubleshooting, unusual noises from a fan module 927
Troubleshooting, unusual noises from a power supply 927
Troubleshooting, unusual odors 928
Troubleshooting, visible physical damage 928

U

United States FCC Class A notice 988
Unusual noises, fan module 927
Unusual noises, power supply 927
Unusual odors, troubleshooting 928
upgradeable microcode 7
User labels 54

V

Visible physical damage 928

W

weight 7
X

X-architecture technology  1