# Lenovo Chassis Management Module 2
# Command-Line Interface Reference Guide

**Note**

Before using this information and the product it supports, read the general information in Appendix B "Notices" on page 491, the *Warranty Information* document, and the *Safety Information* and the *Environmental Notices and User Guide* documents on the Lenovo documentation CD.

**Nineth Edition (May 2019)**

# Contents

# Chapter 1. Introduction

The Lenovo Flex SystemChassis Management Module 2 (CMM) command-line interface (CLI) provides direct access to Flex System management functions as an alternative to using the web-based user interface.

The Lenovo Chassis Management Module 2 supports multiple Flex System chassis types. The CMM automatically detects the chassis type where it is installed. The CMM firmware adjusts the features and command options it supports based on its operating environment.

Using the CLI, you can issue commands to control the power and configuration of the CMM and other components that are in a Flex System chassis. The command-line interface also provides access to the text-console command prompt on each compute node through a Serial over LAN (SOL) connection.

**Notes:**

- Unless otherwise noted, the term "CMM" in this document refers to all CMM types.
- The CMM 2 is also called the CMM II.

You 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 can initiate connections from the client system by using standard remote communication software; no special programs are required. You must authenticate with the CMM before you issue commands. You enter commands one at a time; however, you can use command scripting to enter multiple commands. The CLI does not support keyboard shortcuts, except for the special key sequence, Esc (, that terminates an SOL session.

**Important:** When interfacing with the CMM through an external script-based interface, observe the following restrictions to improve CMM reliability:

- Allow ample time for component discovery after the CMM starts, CMM failover, or addition of new hardware to a Flex System chassis.
- Do not poll the CMM for specific data more than once every 15 minutes.
- Do not run concurrent scripting sessions with the CMM.

The most recent versions of all Lenovo Flex System documentation are available at http://flexsystem.lenovofiles.com/help/index.jsp.

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

## Before you begin

There are some specific hardware and software requirements for using the CMM command-line interface.

**Hardware:**

You do not need any special hardware to use the CMM command-line interface.

You can use the `console` command to control a compute node through SOL (see "console command" on page 107 for information).

**Firmware:**

Make sure that you are using the latest versions of the Unified Extensible Firmware Interface (UEFI) code, system-management processor firmware, diagnostic firmware updates, and device drivers for your compute node, CMM, and other Lenovo Flex System components. Go to http://datacentersupport.lenovo.com for the latest information about upgrading the device drivers, firmware, and UEFI code for Lenovo Flex System components. The latest instructions are in the documentation that comes with the updates.

## Notices and statements in this document

Use this information to understand the most common documentation notices and statements and how they are used.

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

The following notices and statements are used in this document:

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

## Accessibility features for the Lenovo Flex System CMM

Accessibility features help users who have disabilities, such as restricted mobility or limited vision, to use information technology products successfully.

### Accessibility features

Accessibility for the Lenovo Flex SystemCMM interface is provided through the command-line interface. The remote console video feed is not accessible to a screen reader. If you are managing your Lenovo Flex System by using the optional Lenovo XClarity Administrator or Flex System Manager management software, see the documentation for the management device for information about its accessibility features.

The Lenovo Flex System information center is accessibility-enabled. The information center has the following accessibility features:

- Keyboard-only operation.
- Interfaces that are commonly used by screen readers. (The Java access bridge must be installed to make Java applets available to the JAWS screen reader.)
- The attachment of alternative input and output devices.

### Keyboard navigation

This product uses standard Microsoft Windows navigation keys.

### Related accessibility information

You can view the publications for Lenovo Flex System in Adobe Portable Document Format (PDF) by using the Adobe Acrobat Reader. The PDF files are provided on a CD that is packaged with the product, or you can access them through the Lenovo Flex System information center.

### Lenovo and accessibility

See the Accessibility website for more information about the commitment that Lenovo has to accessibility.

# Chapter 2. Command-line interface use and reference

The CMM command-line interface (CLI) provides a convenient method for entering commands that manage and monitor Lenovo Flex System components. This section contains reference information about using the command-line interface.

- "Command-line interface guidelines" on page 5
- "Command targets" on page 6
- "Commands and user authority" on page 10
- "Cabling the CMM" on page 15
- "Starting the command-line interface" on page 17
- "Configuring Lenovo Flex System chassis components by using the CLI" on page 25
- "Configuring the CMM for CLI operation" on page 26
- "Serial over LAN" on page 28
- "Specifying a URL for file transfer" on page 29
- "External authentication of certificates" on page 30

See Chapter 3 "Command reference" on page 37 for detailed information about commands that are used to monitor and control Lenovo Flex System components. Command-line interface error messages are in Chapter 4 "Error messages" on page 407. See the documentation for your operating system for information about commands that you can enter through a Serial over LAN (SOL) connection.

## Command-line interface guidelines

All CMM CLI commands follow the same general syntactical guidelines.

All commands have the following basic structure:

```
command -option parameter
```

Some commands do not require options, and some command options do not require parameters. You can add multiple options to a command on one line to avoid repeating the same command. Options that display a value and options that set a value must not be used together in the same command. The following examples illustrate valid command option syntax:

- `command`
- `command -option_set`
- `command -option_set parameter`
- `command -option1_set parameter -option2_set parameter`

The information for each option is returned in the order in which it was entered and is displayed on separate lines.

Observe the following general guidelines when you use the command-line interface:

- Case sensitivity All commands, command options, and predefined command option parameters are case sensitive.

  **Note:** If you receive a `Command not found` error, make sure that you are typing the command in the correct case. For a list of valid commands, type `help` or `?`.

- Data types The ip_address data type uses a predefined formatted string of `xxx.xxx.xxx.xxx`, where `xxx` is a number from 0 to 255.
- Delimiters
  - Options are delimited with a minus sign.
  - In a command that requires parameters, a single space is expected between an option and its parameter. Any additional spaces are ignored.
- Output format
  - Failed commands generate failure messages.
  - Successful commands are indicated by the message `OK` or by the display of command results.
- Strings
  - Strings that contain spaces must be enclosed in quotation marks, for example, `snmp -cn "John B. Doe"`.
  - String parameters can be mixed case.
- The `help` command lists all commands and a brief description of each command. You can also issue the `help` command by typing `?`. Adding the `-h` parameter to any command displays its syntax.
- You can use the Up Arrow and Down Arrow keys in the command-line interface to access the last eight commands that you entered.

## Command targets

You can set a persistent command target for the CMM CLI or send individual CLI commands to a specific target.

You can use the command-line interface to target commands to the Flex System chassis, the CMM, or to other devices installed in the chassis. The command-line prompt indicates the persistent command environment: the target where commands are directed unless another target is specified. You can specify a command target by using the full target name or by using a target name that is relative to the persistent command environment.

When a command-line interface session is started, the persistent command environment is `system` ; this indicates that commands are being directed to the Flex System chassis.

The following table lists Flex System components that are supported as command targets. Target names have been selected to maintain scripting compatibility with other Lenovo systems.

To direct commands to a specific command target, its path name must be specified, either as a full path name or as a path name based on the current persistent command environment. To view path names for targets in your Flex System chassis, use the “list command” on page 224.

*Table 1. Valid command targets*

| Component | Target path |
|---|---|
| Flex System chassis | `system` |
| CMM (by bay number) | `mm[`*x*`]` |
| CMM (primary) | `mm[p]` or `mm[P]` |
| CMM (standby) | `mm[s]` or `mm[S]` |
| Compute node | `blade[`*x*`]` |
| Logical node grouping | `bladegroup[x]` |

*Table 1. Valid command targets (continued)*

| Component | Target path |
|---|---|
| System-management processor | `sp` |
| Expansion adapter | `exp[`*x*`]` |
| Compute node management card | `mgmtcrd[`*x*`]` |
| Compute node microprocessor | `cpu[`*x*`]` |
| Expansion node | `be[`*x*`]` |
| Compute node high-speed expansion card | `hsec[`*x*`]` |
| Compute node memory | `memory[`*x*`]` |
| Compute node flash DIMM (Lenovo eXFlash Storage DIMM) | `flashdimm[`*x*`]` |
| Storage expansion enclosure | `bladeenclosure[`*x*`]` |
| Storage disk | `disk[`*x*`]` |
| Alarm panel | `tap[`*x*`]` |
| Storage backplane | `stgbkplane[`*x*`]` |
| Add-in card | `addin[`*x*`]` |
| Add-in card PCI-Express module | `pciexpress[`*x*`]` |
| I/O (switch) module | `switch[`*x*`]` |
| Power supply | `power[`*x*`]` |
| Fan logic module | `fanmux[`*x*`]` |
| Fan module | `blower[`*x*`]` |
| Rear LED card | `mt[`*x*`]` |

You can change the persistent command environment for the remainder of a command-line interface session by using the `env` command (see "env command" on page 131). When you list the target as a command attribute by using the `-T` option, you change the target environment for the command that you are entering, temporarily overriding the persistent command environment. You can specify target environments by using the full path name or by using a partial (relative) path name that is based on the persistent command environment. Full path names always begin with "system". The levels in a path name are divided using a colon ( : ).

For example:

- Use the `-T system:mm[1]` option to redirect a command to the CMM in bay 1.
- Use the `-T system:switch[1]` option to redirect a command to the I/O module in I/O bay 1.
- Use the `-T sp` option to redirect a command to the system-management processor in the compute node in node bay 3, when the persistent command environment is set to the compute node in node bay 3.
- Use the `-T bladegroup[1]:blade[1]` option to redirect a command to the first compute node in a logical node grouping in node bay 1, when the persistent command environment is set to the Flex System chassis.

Most CMM commands must be directed to the primary CMM. If only one CMM is installed in the Flex System chassis, it always acts as the primary CMM. Either CMM can function as the primary CMM; however, only one CMM can be primary at one time. You can determine which CMM is acting as the primary CMM by using the `list` command (see "list command" on page 224).

Commands can be directed to the primary CMM, regardless of its bay location, using the `-T system:mm[p]` or `-T system:mm[P]` option. Commands can be directed to the standby CMM, regardless of its bay location, using the `-T system:mm[s]` or `-T system:mm[S]` option.

**Example:** To display a hierarchical list of all command targets in the Flex System chassis, while the chassis is set as the persistent command environment, at the `system>` prompt, type

```
list -l a
```

The following example shows the information that might be returned when the command is run:

```
system> list -l a
system
        blade[1]  Server1
            sp
            cpu[1]
            tap[1]
            stgbkplane[1]
            be[1]
                addin[1]
                    hsec[2]
                addin[2]
            memory[1]
            memory[4]
            addin[1]
        blower[1]
        blower[2]
        blower[5]
        blower[6]
        blower[7]
        blower[10]
        power[1]
                blower[1]
        power[2]
                blower[1]
        mm[1]      standby
        mm[2]      primary
        switch[1]
        mt[1]
        fanmux[1]
        fanmux[2]
system>
```

The following table shows each target with its full path. This is the path that would be used if the persistent command environment was set to the Flex System chassis.

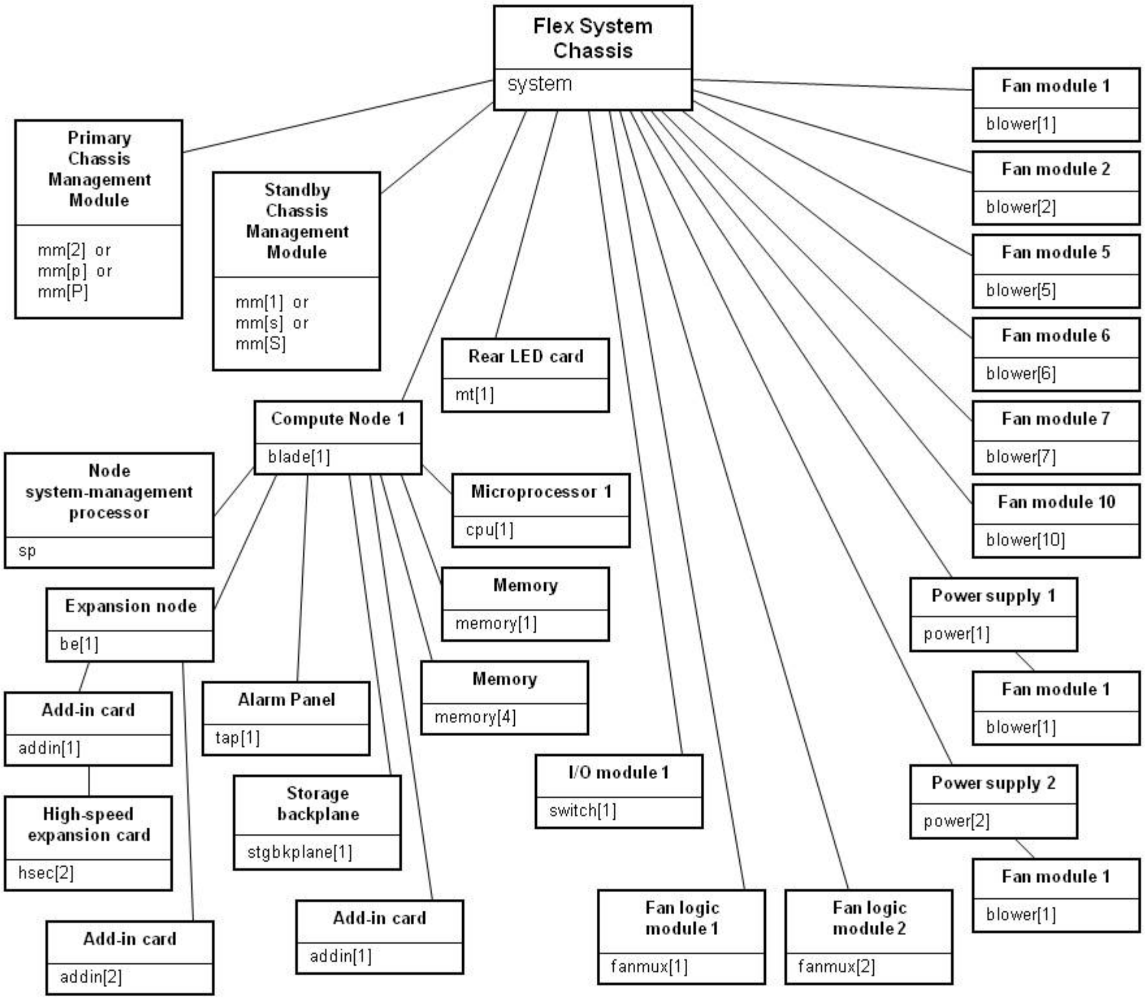
*Table 2. Example system components and command paths*

| Component | Target path |
|---|---|
| Flex System chassis | `system` |
| Compute node, bay 1 (named Server1) | `system:blade[1]` |
| Node system-management processor, compute node bay 1 | `system:blade[1]:sp` |
| Microprocessor, compute node bay 1 | `system:blade[1]:cpu[1]` |
| Alarm panel, compute node bay 1 | `system:blade[1]:tap[1]` |

*Table 2. Example system components and command paths (continued)*

| Component | Target path |
|---|---|
| Storage backplane, compute node bay 1 | `system:blade[1]:stgbkplane[1]` |
| Expansion node 1, compute node bay 1 | `system:blade[1]:be[1]` |
| Add-in card 1, expansion node 1, compute node bay 1 | `system:blade[1]:be[1]:addin[1]` |
| High-speed expansion card 2, add-in card 1, expansion node 1, compute node bay 1 | `system:blade[1]:be[1]:addin[1]hsec[2]` |
| Add-in card 2, expansion node 1, compute node bay 1 | `system:blade[1]:be[1]:addin[2]` |
| Memory module 1, compute node bay 1 | `system:blade[1]:memory[1]` |
| Memory module 4, compute node bay 1 | `system:blade[1]:memory[4]` |
| Add-in card 1, compute node bay 1 | `system:blade[1]addin[1]` |
| Fan module 1 | `system:blower[1]` |
| Fan module 2 | `system:blower[2]` |
| Fan module 5 | `system:blower[5]` |
| Fan module 6 | `system:blower[6]` |
| Fan module 7 | `system:blower[7]` |
| Fan module 10 | `system:blower[10]` |
| Power supply 1 | `system:power[1]` |
| Fan module, power supply 1 | `system:power[2]:blower[1]` |
| Power supply 2 | `system:power[2]` |
| Fan module, power supply 2 | `system:power[2]:blower[1]` |
| Standby CMM, CMM bay 1 | `system:mm[s]` or `system:mm[S]` or `system:mm[1]` |
| Primary CMM, CMM bay 2 | `system:mm[p]` or `system:mm[P]` or `system:mm[2]` |
| I/O (switch) module, bay 1 | `system:switch[1]` |
| Rear LED card | `system:mt[1]` |
| Fan logic module 1 | `system:fanmux[1]` |
| Fan logic module 2 | `system:fanmux[2]` |

The complete command target hierarchy for the example is shown in the following illustration.



## Commands and user authority

Some CMM CLI commands can be executed only by users who are assigned a required level of authority.

Users are assigned authority levels according to user permission groups that are set up for the CMM.

Users with Supervisor command authority can execute all commands. Commands that display information do not require any special command authority; however, users can be assigned restricted read-only access, as follows:

- Users with Operator command authority can execute all commands that display information.
- Users with Chassis Operator custom command authority can execute commands that display information about the common Flex System chassis components.
- Users with Blade Operator custom command authority can execute commands that display information about the node devices, such as compute nodes.
- Users with Switch Operator custom command authority can execute commands that display information about the I/O modules.

Table 3 “Command authority relationships” on page 11 shows the command-line interface commands and their required authority levels. To use the table, observe the following guidelines:

- The commands in this table apply only to the command variants that set values or cause an action and require a special command authority: display variants of the commands do not require any special command authority.
- If a command requires only one command authority at a time, each of the applicable command authorities is indicated by a dot (•). If a command requires a combination of two or more command authorities, the applicable command authorities are indicated by a ◊. For example, the cin command is available to a user with the Supervisor command authority and to a user with both the Chassis Account Management and Chassis Configuration command authorities.

**Important:** Users and permission groups for the Flex System chassis are controlled by the CMM in each chassis, using the CMM CLI “users command” on page 372 and the “permgroups command” on page 238 or the CMM web interface. If your Flex System configuration includes the optional Lenovo XClarity Administrator or Flex System Manager management node, users and permission groups for each optional management device are controlled by the optional management software (see http://flexsystem.lenovofiles.com/help/topic/com.lenovo.lxca.doc/aug_product_page.html for information about the Lenovo XClarity Administrator or http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.8731.doc/product_page.html for information about the Flex System Manager).

**Notes:**

1. LDAP authority levels are not supported by the CMM web interface. If you enable the enhanced role-based security using the CMM web interface, you must configure the external LDAP server using an LDAP snap-in tool that is available for Microsoft Windows operating systems.
2. To use the LDAP authority levels, you must make sure that the version of LDAP security that is used by the CMM is set to v2 (enhanced role-based security model). See “ldapcfg command” on page 211 for information.

*Table 3. Command authority relationships*

| | **Command Authority** | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Command** | **Supervisor** | **Chassis Account Management** | **Chassis Log Management** | **Chassis Administration** | **Chassis Configuration** | **Blade Administration** | **Blade Configuration** | **Blade Remote Presence** | **I/O Module Administration** | **I/O Module Configuration** |
| accesscontrol | • | • | • | • | • | • | • | • | • | • |
| accseccfg | • | | | | • | | | | | |
| advfailover | • | | | | • | | | | | |
| airfilter | • | • | • | • | • | | | | | |
| alarm<br>(system, CMM, power supply, or blower target) | • | | | | • | | | | | |
| alarm<br>(compute node target) | • | | | | | | • | | | |

*Table 3. Command authority relationships (continued)*

| Command | Command Authority | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Supervisor | Chassis Account Management | Chassis Log Management | Chassis Administration | Chassis Configuration | Blade Administration | Blade Configuration | Blade Remote Presence | I/O Module Administration | I/O Module Configuration |
| alarm<br>(I/O module target) | · | | | | | | | | | · |
| alertcfg | · | | | | · | | | | | |
| alertentries | · | · | · | · | · | | | | | |
| baydata | · | | | | | | · | | | |
| bootmode | · | | | | | | · | | | |
| chconfig | · | | | | · | | | | | |
| chlog | · | | | | · | | | | | |
| chmanual | · | · | · | · | · | · | · | · | · | · |
| cimsub | · | | | | · | | | | | |
| cin | · | ◊ | | | ◊ | | | | | |
| clear | · | | | ◊ | ◊ | | | | ◊ | ◊ |
| clearlog | · | | · | | | | | | | |
| config<br>(compute node target) | · | | | | | | · | | | |
| config<br>(CMM or system target) | · | | | | · | | | | | |
| console | · | | | | | | | · | | |
| crypto | · | | | | · | | | | | |
| date | · | | | | · | | | | | |
| dns | · | | | | · | | | | | |
| events -che | · | · | · | · | · | · | · | · | · | · |
| events -che -add -rm | · | | | | · | | | | | |
| files -d | · | | | · | · | · | · | | · | · |
| fsmcm | · | · | | | | | | | | |
| fuelg | · | | | | · | | | | | |
| groups | · | | | | · | | | | | |
| ifconfig (compute node target) | · | | | | | | · | | | |

*Table 3. Command authority relationships (continued)*

| Command | Command Authority | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Supervisor | Chassis Account Management | Chassis Log Management | Chassis Administration | Chassis Configuration | Blade Administration | Blade Configuration | Blade Remote Presence | I/O Module Administration | I/O Module Configuration |
| ifconfig (compute node ISMP, CMM, and system targets) | • | | | | • | | | | | |
| ifconfig (I/O module target) | • | | | | | | | | | • |
| ifconfig -pip (I/O module target) | • | | | | | | | | • | • |
| ldapcfg | • | | | | • | | | | | |
| led -info, -loc<br>(system target) | • | | | • | | | | | | |
| led -info, -loc<br>(compute node target) | • | | | | | • | | | | |
| led -loc<br>(I/O module target) | • | | | | | | | | • | |
| monalerts | • | | | | • | | | | | |
| ntp | • | | | | • | | | | | |
| permgroups | • | | • | | | | | | | |
| pmpolicy | • | | | | • | | | | | |
| portcfg | • | | | | • | | | | | |
| ports | • | | | | • | | | | | |
| ports (I/O module target) | | | | | | | | | | • |
| power -on, -off, -softoff, -cycle | • | | | | | • | | | • | |
| power -on -c, -cycle -c | • | | | | | ◊ | | ◊ | | |
| power -ap, -aux, -d | • | | | | • | | • | | | |
| power -local, -wol | • | | | | | | • | | | |
| pwrprofile | • | • | • | • | • | | | | | |
| read[1] | • | | | | • | | | | | |
| reset<br>(compute node or ISMP target) | • | | | | | • | | | | |
| reset<br>(I/O module target) | • | | | | | | | | • | |
| reset<br>(CMM target) | • | | | • | | | | | | |

*Table 3. Command authority relationships (continued)*

|  | Command Authority | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Command** | **Supervisor** | **Chassis Account Management** | **Chassis Log Management** | **Chassis Administration** | **Chassis Configuration** | **Blade Administration** | **Blade Configuration** | **Blade Remote Presence** | **I/O Module Administration** | **I/O Module Configuration** |
| reset -c, -sft,<br>(compute node target) | • | | | | | ◊ | | ◊ | | |
| reset -exd, -full, -std<br>(I/O module target) | • | | | | | | | | • | |
| reset -f, -standby<br>(CMM target) | • | | | • | | | | | | |
| sddump | • | | | | | • | | | | |
| sdemail | • | • | • | • | • | • | • | • | • | • |
| security | • | | | | • | | | | | |
| service<br>(CMM target) | • | | | • | • | | | | | |
| service<br>(compute node or storage node target) | • | | | | | • | • | | | |
| service<br>(compute node system-management processor target) | • | | | | | | • | | | |
| service<br>(I/O module target) | • | | | | | | | | • | |
| smtp | • | | | | • | | | | | |
| snmp | • | | | | • | | | | | |
| sol | • | | | | • | | • | | | |
| sshcfg | • | | | | • | | | | | |
| sslcfg | • | | | | • | | | | | |
| syslog | • | • | • | • | • | | | | | |
| tcpcmdmode | • | | | | • | | | | | |
| trespass | • | | | | • | | | | | |
| uicfg | • | | | | • | | | | | |
| update (CMM target) | • | | | • | | | | | | |
| update (I/O module target) | • | | | | | | | | • | |
| uplink | • | | | | • | | | | | |

*Table 3. Command authority relationships (continued)*

| | Command Authority | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Command** | **Supervisor** | **Chassis Account Management** | **Chassis Log Management** | **Chassis Administration** | **Chassis Configuration** | **Blade Administration** | **Blade Configuration** | **Blade Remote Presence** | **I/O Module Administration** | **I/O Module Configuration** |
| users | • | • | | | | | | | | |
| vlan (CMM target) | • | | | | • | | | | | |
| vlan (system target) | • | | | | | | • | | | |

**Notes:**

1. To successfully restore all settings, a user running the `read` command must have permission to modify any settings controlled by individual commands in the configuration being restored.

## Cabling the CMM

You can cable the CMM to support a management connection that best matches your site configuration.

You must connect a client system to the CMM to configure and manage operation of a Flex System chassis. The CMM supports Ethernet (local or remote) and serial management connections.

You can manage a Flex System chassis by using the CMM command-line interface that you access through Telnet or through the serial-management connector. You can also use the CMM web interface, which you access through the remote management and console (Ethernet) connector, to manage Flex System chassis devices. Use an SOL session through the CMM command-line interface, to access the operating system text console of a compute node or the system-management processor of compute nodes that have a Unified Extensible Firmware Interface (UEFI).

To access the CMM management interfaces, you need the following equipment and information:

- For connection through the CMM web interface:
  - A system with Ethernet connection capability. To facilitate connections at multiple locations, you can use a notebook computer.
  - The CMM IP address (the default CMM IP address is 192.168.70.100).
  - For networked connection to the CMM, a standard Ethernet cable and a local Ethernet network port (facility connection).
  - For direct connection of a system to the CMM remote management and console (Ethernet) connector, a standard Ethernet cable or an Ethernet crossover cable.
- For connection through the CMM CLI:
  - A system with Ethernet or serial connection capability. To facilitate connections at multiple locations, you can use a notebook computer.
  - The CMM MAC address (listed on the label on the CMM).

- For networked connection to the CMM, a standard Ethernet cable and a local Ethernet network port (facility connection).
- For direct connection of a system to the CMM remote management and console (Ethernet) connector, a standard Ethernet cable or an Ethernet crossover cable.
- For serial connection of a system to the CMM mini-USB serial-management connector, a serial cable.

The following topics describe how to cable to the CMM to configure and manage a Flex System chassis.

## Networked connection

You can use an Ethernet cable to connect the CMM to a management network.

To connect an Ethernet cable to the CMM for management network connection, complete the following steps:

Step 1. Connect one end of a Category 5 or higher Ethernet cable to the Ethernet connector of the CMM.

Step 2. Connect the other end of the Ethernet cable to the management network.

Step 3. Check the Ethernet LEDs on the CMM to make sure that the network connection is working. (See "CMM controls and indicators" in *Lenovo Chassis Management Module 2 Installation Guide* for Ethernet LED locations.)

- When the green Ethernet port link LED is lit, there is an active connection through the port to the network.
- When the green Ethernet port active LED is flashing, it indicates that there is activity through the port over the network link.

## Direct client connection

You can use an Ethernet cable to connect the CMM directly to a client computer.

To connect a client computer directly to the CMM by using an Ethernet cable, complete the following steps.

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

Step 1. Connect one end of a Category 5 or higher Ethernet cable or a Category 5 or higher Ethernet crossover cable to the Ethernet connector of the CMM.

Step 2. Connect the other end of the cable to the Ethernet connector on the client system.

Step 3. Check the Ethernet LEDs on the CMM to make sure that the network connection is working. (See "CMM controls and indicators," in the *Lenovo Chassis Management Module 2 Installation Guide*, for Ethernet LED locations.)

- When the green Ethernet port link LED is lit, there is an active connection through the port to the network.
- When the green Ethernet port active LED is flashing, it indicates that there is activity through the port over the network link.

## Serial cable connection

You can use a serial cable to connect the CMM to a client computer or a serial-management network.

See "CMM serial port pin assignments," in the *Lenovo Chassis Management Module 2 Installation Guide*, for serial-management connector pin assignments.

**Note:** An optional cable kit with adapters is available to convert the CMM mini-USB connector for RJ-45, DB-9, or standard USB cable connection. See http://static.lenovo.com/us/en/serverproven/index.shtml for available Lenovo Flex System options.

To connect a serial cable to the CMM for a management connection, complete the following steps:

Step 1. Connect one end of a serial cable to the mini-USB serial-management connector on the CMM.

Step 2. Connect the other end of the serial cable to the serial connector on the client system, such as a notebook computer, or to a serial-management network.

Step 3. Configure the serial device that the CMM connects to as follows:

a. Baud rate = 115200

b. Parity = none

c. Stop bits = 1

## Starting the command-line interface

Access the CMM command-line interface from a client system through a Telnet, Secure Shell (SSH), or serial connection.

You can access the command-line interface through an Ethernet connection by establishing a Telnet session with the IP address of the CMM or by establishing a Secure Shell (SSH) session. You can also access the command-line interface by using a serial connection. You can establish up to 20 separate Telnet, serial, or SSH sessions to the CMM, giving you the ability to have 20 active command-line interface sessions at the same time.

Although a remote network administrator can access the CMM command-line interface through Telnet, this method does not provide a secure connection. As a secure alternative to using Telnet to access the command-line interface, use a serial or SSH connection. SSH ensures that all data that is sent over the network is encrypted and secure. You cannot access the CMM CLI through Telnet while using the Secure chassis security policy setting.

The following SSH clients are available. Although some SSH clients have been tested, support or nonsupport of any particular SSH client is not implied.

- The SSH clients that are distributed with operating systems such as Linux, AIX, and UNIX (see your operating-system documentation for information). The SSH client of Red Hat Linux 8.0 Professional was used to test the command-line interface.
- The SSH client of cygwin (see http://www.cygwin.com for information).
- Putty (see http://www.chiark.greenend.org.uk/~sgtatham/putty for information).

The following table shows the types of encryption algorithms that are supported, depending on the client software version that is being used.

| **Algorithm** | **SSH version 2.0 clients** |
|---|---|
| Public key exchange | Diffie-Hellman-group 1-sha-1 |
| Host key type | DSA - 2048-bit |
| Bulk cipher algorithms | 3-des-cbc or blowfish-cbc |
| MAC algorithms | Hmac-sha1 |

The following topics describe how to connect your system to the CMM to perform initial configuration of the Flex System chassis. The CMM has the following default settings.

**Note:** By default, the CMM does not have a fixed static IPv6 IP address. For initial access to the CMM in an IPv6 environment, you can use the IPv4 IP address or the IPv6 link-local address. See “IPv6 addressing for initial connection” on page 19 for information about determining IPv6 addressing for initial connection.

- IPv4 IP address: 192.168.70.100 (primary and secondary CMM)
- IPv4 Subnet: 255.255.255.0
- User ID: USERID (all capital letters)
- Password: PASSW0RD (note the number zero, not the letter O, in PASSW0RD)

For IPv4, the system that you are connecting to the CMM must be configured to operate on the same subnet as the CMM. If the IP address of the CMM is outside of your local domain, you must change the Internet Protocol properties on the system that you are connecting.

**Note:** The available password options depend on the password options that are configured for the Flex System chassis.

## CMM network access tag

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

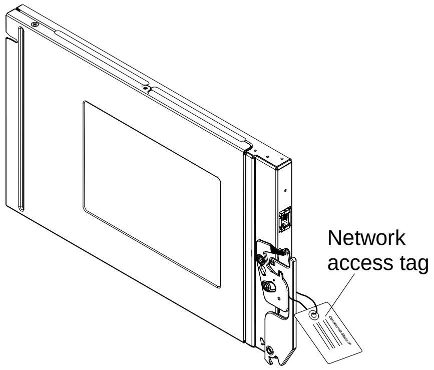
**Important:** Remove the network access tag from the CMM, before you install the CMM in a Flex System chassis.

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)

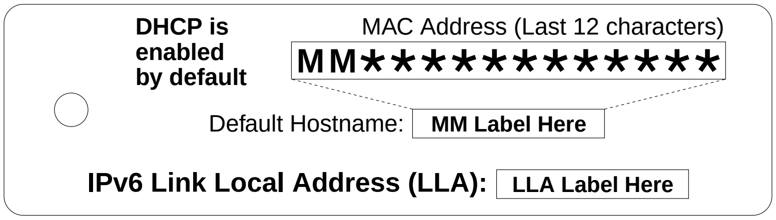
The network access tag is attached to the front of the CMM, as shown in the following illustration.

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



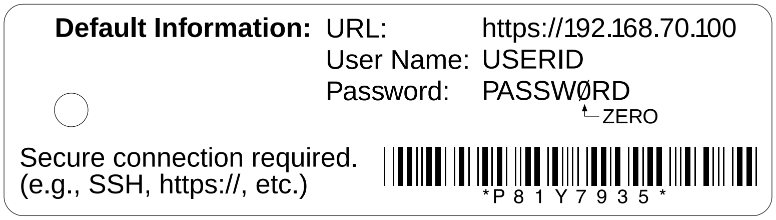
The front of the network access tag lists the CMM MAC address, default host name, and IPv6 link local address (LLA), as shown in the following illustration.

**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 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: PASSWØRD
ZERO
Secure connection required.
(e.g., SSH, https://, etc.)
*P 8 1 Y 7 9 3 5 *

## IPv6 addressing for initial connection

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

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

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

- Read the CMM link-local address on the network access tag that is attached to the front of the CMM (see "CMM network access tag" on page 18 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" on page 174 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 MM*xxxxxxxxxxxx*, where *xxxxxxxxxxxx* is the MAC address. For example:

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

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

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

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

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

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

- `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-CBD0`

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

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

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

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

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

## Telnet connection

You can connect to the CMM CLI through a Telnet session.

**Note:** The Telnet connection is not available when the CMM security policy is set to Secure (the manufacturing default setting).

After you connect an Ethernet cable from the client computer to the CMM (direct connection or through a network), complete the following steps:

Step 1. Make sure that the subnet of the client computer is set to the same value as the CMM (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. To connect to the CMM for the first time, you might have to change the Internet Protocol properties on the client computer.

Step 2. From a command prompt on the client computer, type `telnet` *ip_address* (where *ip_address* is the CMM IP address), and press Enter. 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 manufacturing default static IPv4 IP address is 192.168.70.100, the default IPv4 subnet address is 255.255.255.0, and the default host name is MM*xxxxxxxxxxxx*, where *xxxxxxxxxxxx* is the burned-in MAC address. The MAC address is on a label on the CMM, below the reset button (see "CMM controls and indicators," in the *Lenovo Chassis Management Module 2 Installation Guide*, for the location of the reset button). See “IPv6 addressing for initial connection” on page 19 for information about determining IPv6 addressing for initial connection.

Step 3. At the login prompt, type the CMM user ID. At the password prompt, type the CMM password.

- The same user ID and password are used for all methods of connecting to the CMM. The password is case sensitive. The user ID is *not* case sensitive.

- The default CMM user name is USERID, and the default password is PASSW0RD (note the number zero, not the letter O, in PASSW0RD).

The CLI command prompt is displayed. You can now enter commands for the CMM.

Step 4. If you are connecting to the CMM for the first time, perform the initial configuration of the Flex System chassis (see "Configuring the CMM," in the *Lenovo Chassis Management Module 2 Installation Guide*, for information).

## Serial connection

You can connect to the CMM CLI through a serial connection.

After you connect the serial cable from the CMM to the client computer, complete the following steps:

Step 1. Make sure that the serial port settings of the client system match the settings of the serial port on the CMM.The default CMM serial port settings are as follows:

- Baud rate (BPS): 115200
- Data bits: 8
- Parity: no parity
- Stop bits: 1
- Flow control: none

Step 2. If any of the serial port settings for the client system were changed, reset the CMM.

Reset the CMM manually by pressing the reset button (see "CMM controls and indicators," in the *Lenovo Chassis Management Module 2 Installation Guide*, for the location of the reset button).

**Attention:** If you push the paper clip in all the way and hold it for approximately 10 seconds, the CMM is reset to the default configuration.

Reset the CMM by using the CMM CLI **reset** command (see “reset command” on page 289 for information about command use).

Reset the CMM by using the CMM web interface by selecting **Restart** from the **Mgt Module Management** menu. All fields and options are fully described in the CMM web interface online help.

Step 3. Open a terminal emulator window on the client computer and establish a connection to the CMM serial port.

Step 4. At the login prompt, type the CMM user ID. At the password prompt, type the CMM password.

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

The CLI command prompt is displayed. You can now enter commands for the CMM.

Step 5. If you are connecting to the CMM for the first time, perform the initial configuration of the Flex System chassis (see "Configuring the CMM," in the *Lenovo Chassis Management Module 2 Installation Guide*, for information).

## Secure Shell (SSH) connection

You can connect to the CMM CLI through a Secure Shell (SSH) connection.

After you connect an Ethernet cable from the client computer to the CMM (direct connection or through a network), complete the following steps:

Step 1. Make sure that the SSH server on the Lenovo Flex SystemCMM is enabled (SSH is enabled by default).

- In the CMM web interface:
  - Set the SSH port on the Port Assignments 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.
  - Enable the SSH server on the SSH Server page on the Security page (select **Security** from the **Mgt Module Management** menu). All fields and options are fully described in the CMM web interface online help.
- In the CMM CLI:
  - Set the SSH port by using the **ports -sshe** command (see “ports command” on page 250 for information about command use).
  - Enable the SSH server by using the **sshcfg -cstatus** command (see “sshcfg command” on page 326 for information about command use).

Step 2. Start an SSH session to the CMM by using the SSH client of your choice. For example, if you are using the cygwin client, from a command prompt on the network-management workstation, type `ssh` *ip_address* (where *ip_address* is the CMM IP address), and press Enter. 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 manufacturing default static IPv4 IP address is 192.168.70.100, the default IPv4 subnet address is 255.255.255.0, and the default host name is MM*xxxxxxxxxxxx*, where *xxxxxxxxxxxx* is the burned-in MAC address. The MAC address is on a label on the CMM, below the reset button. See “IPv6 addressing for initial connection” on page 19 for information about determining IPv6 addressing for the initial connection.

Step 3. At the login prompt, type the CMM user ID. At the password prompt, type the CMM password.

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

The CLI command prompt is displayed. You can now enter commands for the CMM.

Step 4. If you are connecting to the CMM for the first time, perform the initial configuration of the Flex System chassis (see "Configuring the CMM," in the *Lenovo Chassis Management Module 2 Installation Guide*, for information).

## Using the Secure Shell (SSH) server

There are several ways that you can use the CMM Secure Shell (SSH) server.

The following SSH clients are available. Although some SSH clients have been tested, support or nonsupport of any particular SSH client is not implied.

- The SSH clients that are distributed with operating systems such as Linux, AIX, and UNIX (see your operating-system documentation for information).
- The SSH client of cygwin (see http://www.cygwin.com for information).

For information about using the CMM CLI to configure your system for SSH operation by using the `sshcfg` command, see “sshcfg command” on page 326.

If you are using the Secure Shell client that is based on OpenSSH, such as the client that is included in Red Hat Linux version 7.3, to start an interactive command-line Secure Shell session to a CMM with network address 192.168.70.2, type a command similar to the following example:

```
ssh -x -l USERID 192.168.70.2
```

where `-x` indicates no X Window System forwarding and `-l` indicates that the session is to use the login ID USERID.

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

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

If the CLI command requires special characters such as quotation marks, you must escape them so that they are not consumed by the command shell on your client system. For example, to set a new trespass warning, type a command similar to the following example:

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

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

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

## SSH CLI exit codes

The SSH CLI commands return exit codes.

All CLI commands that are run in an SSH client single-command environment provide exit codes to indicate their outcomes. The following table shows exit codes that are supported; other exit codes are reserved for future use.

*Table 4. SSH CLI exit codes*

| Name | Value (decimal) | Description |
|---|---|---|
| EX_OK | 0 | Successful command execution. |
| EX_USAGE | 64 | Command-line usage error: syntax error, wrong command arguments or number of arguments, or invalid command target. |
| EX_DATAERR | 65 | Input data error: invalid configuration file or SSH key parsing error. |
| EX_NOINPUT | 66 | The input file does not exist or is not readable. |
| EX_UNAVAILABLE | 69 | The command-line interface is not available: CLI oversubscribed, CLI disabled, or the data returned by a command has an unexpected value. |
| EX_SOFTWARE | 70 | Internal software error. Check the CMM event log for other error indications. |
| EX_TEMPFAIL | 75 | The command could not perform a write operation because the device or CMM was not in the correct state. Check for conflicting tasks or conditions and try to run the command again. |

*Table 4. SSH CLI exit codes (continued)*

| Name | Value (decimal) | Description |
|---|---|---|
| CLI_ERR_NOT_ AUTHORIZED | 126 | Authorization error: the user does not have sufficient privileges to execute the command. |
| CLI_ERR_CNF | 127 | Command not found. |

## CMM ports

The Lenovo Chassis Management Module 2 modules use a variety of TCP/IP ports for communication. This topic lists these ports and indicates the ones that are fixed or can be changed by an administrator. You need to make sure that your network allows communications through these ports for the Lenovo Chassis Management Module 2 modules to function and communicate correctly.

**Notes:** The CMM HTTP and HTTPS ports are open at all times. Port behavior is determined by the CMM HTTPS port setting, which can be affected by the CMM chassis security policy setting:

- When the CMM HTTPS port is enabled, the HTTP port (port 80) remains open and redirects to the HTTPS port (port 443). When the chassis security policy is set to secure, the CMM HTTPS port is automatically enabled and its setting cannot be changed.
- When the CMM HTTPS port is disabled, the HTTPS port (port 443) remains open and redirects to the HTTP port (port 80).

*Table 5. User configurable Lenovo Flex System Enterprise Chassis ports*

| Port name | Port number | Description |
|---|---|---|
| CIM/XML HTTPS | 5989 (default) | CIM/XML HTTPS used by management applications |
| FTP | 21 (default) | FTP |
| FTP Data | 20 (default) | FTP Data |
| http | 80 (default) | Web server HTTP connection - TCP |
| https | 443 (default) | SSL connection for HTTP-TCP |
| Secure TCP Command Mode | 6091 (default) | Secure TCP Command Mode used by management applications |
| SLP | 427 (default) | Service location protocol - UDP |
| SNMP agent | 161 (default) | SNMP get/set commands - UDP |
| SNMP traps | 162 (default) | SNMP traps |
| SSH | 22 (default) | Secure Shell (SSH) command-line interface - TCP |
| TCP Command Mode | 6090 (default) | TCP Command Mode |

Table 5. User configurable Lenovo Flex System Enterprise Chassis ports (continued)

| Port name | Port number | Description |
|---|---|---|
| telnet | 23 (default) | Telnet command-line interface connection -TCP |
| TFTP | 69 (default) | TFTP |

**Note:** The LDAP server port (port 389) is used only with the STARTTLS protocol extension to provide an equivalent to LDAPS port 636. Unsecure access to the LDAP server port is disabled: if a secure SSL connection is not established, connection to port 389 is refused. Port 389 is the default port for the CMM internal interface. Port 636 the default port for the CMM external interface.

Table 6. Fixed Lenovo Flex System Enterprise Chassis ports

| Port number | Description |
|---|---|
| 25 | E-mail alerts - TCP |
| 53 | DNS resolver - UDP |
| 67 and 68 | DHCP - UDP |
| 123 | NTP |
| 389 | LDAP server port |
| 547 | DHCP (IPv6) - UDP |
| 623 | RMCP (Remote Management and Control Protocol) |
| 636 | LDAPS (secure LDAP) |
| 830 | NETCONF (Network Configuration Protocol)<br>**Note:** If an I/O module supports the NETCONF protocol, port 830 is open by default. |

## Configuring Lenovo Flex System chassis components by using the CLI

You must configure the Lenovo Flex System chassis and its components for your operating environment. You can perform this configuration by using the CMM command-line interface.

The Lenovo Flex System chassis automatically detects the modules and compute nodes that are installed and stores the vital product data (VPD). When the chassis is started, the CMM automatically configures the remote management and console (Ethernet) connector of the CMM, so that you can configure and manage Lenovo Flex System components. You configure and manage Lenovo Flex System components remotely by using the CMM command-line interface (CLI) or the CMM web interface. The CMM web interface includes an initial setup wizard that simplifies the setup operation (see "Using the Initial Setup Wizard" in the *Lenovo Chassis Management Module 2 User*'s *Guide* for information). The optional Lenovo XClarity Administrator or Flex System Manager software also supports selected configuration and management functions for the Lenovo Flex System chassis.

To manually configure the basic settings for an Lenovo Flex System chassis by using the CMM CLI, complete the following steps:

Step 1. Configure the CMM to use the CLI (see "Configuring the CMM for CLI operation" on page 26 for information).

Step 2. Start a CMM CLI session (see "Starting the command-line interface" on page 17 for information).

Step 3. View the installed components in the Lenovo Flex System chassis and their health status by using the `list` command (see "list command" on page 224 for information) and `health` command (see "health command" on page 164 for information). All components in the chassis should be shown and indicate a healthy state.

Step 4. Verify that the general settings of the CMM are correct by using the `config` command (see "config command" on page 102 for information).

Step 5. Set the system date and time by using the `date` command (see "date command" on page 113 for information).

Step 6. Verify the CMM IP configuration by using the `ifconfig` command (see "ifconfig command" on page 174 for information).

Step 7. Set up credentials of the main supervisor user account (USERID) by using the `users` command (see "users command" on page 372 for information).

Step 8. To communicate with network resources and with components in the Lenovo Flex System chassis, configure the I/O-module ports.

**Notes:**

- To communicate with the compute nodes for functions such as deploying an operating system or application program over a network, at least one external (in-band) port on an Ethernet switch in one of the I/O bays of the Lenovo Flex System chassis must be configured for operation and connected.
- If a pass-thru module is installed in an I/O bay (instead of an Ethernet I/O module), you might have to configure the network switch that the pass-thru module is connected to; see the documentation that comes with the pass-thru module and the network switch for information and instructions.
- You might be able to configure an I/O module through its external management connector. An Ethernet switch module can be configured through an external port that is enabled for management connection by the CMM. Depending on your I/O module and configuration, configuration can be performed by using a Telnet interface, a serial connection, or a web browser. See the documentation that comes with each I/O module for information and instructions.

a. Enable and configure I/O-module port settings by using the `ports` command (see "ports command" on page 250 for information).

b. Configure IP addresses for the I/O modules by using the `ifconfig` command (see "ifconfig command" on page 174 for information).

Step 9. Set the overall CMM security policy by using the `security` command (see "security command" on page 298 for information).

Step 10. Set the CMM DNS configuration by using the `dns` command (see "dns command" on page 127 for information).

Step 11. Set an email address for CMM event notifications by using the `alertentries` command (see "alertentries command" on page 58 for information).

These steps complete basic configuration of the Lenovo Flex System chassis. You can now perform additional setup operations, as required, for your specific chassis configuration.

## Configuring the CMM for CLI operation

You must configure the CMM to use the command-line interface.

You configure only the primary (active) CMM. If a standby (redundant) CMM is installed, it receives the configuration and status information automatically from the primary CMM when necessary. The configuration information in this topic applies to the primary CMM, which might be the only CMM in the Lenovo Flex System chassis.

If the CMM that you are installing is the only CMM in the Lenovo Flex System chassis and you have a saved CMM configuration file, you can apply the saved configuration file to the replacement CMM. See "read command" on page 280 for information about applying a saved configuration file.

For the primary CMM to communicate, you must configure the IP address for the remote management and console (Ethernet) port (eth0) of the CMM by using the CMM CLI `ifconfig -eth0` command (see "ifconfig command" on page 174 for information about command use). The initial automatic CMM configuration enables a remote console to connect to the CMM to configure the port completely and to configure the rest of the Lenovo Flex System chassis.

After you connect the primary CMM to the network, the Ethernet management port connection is configured in one of the following ways. Either of these actions enables the Ethernet management port on the primary CMM.

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

  **Note:** If the CMM DHCP setting is set to try the DHCP server and then use the static IP address, the CMM uses the static IP address when the DHCP server is not available during CMM startup. When this occurs, the IP address might not be reachable if multiple CMMs were started with the same static IP address. Use the `dhcpinfo` command to view the DHCP settings for the CMM (see "dhcpinfo command" on page 115 for information).

**Important:** You cannot connect to the CMM by using the manufacturing-defined static IP address and manufacturing default subnet address until at least 3 minutes after CMM startup.

**Note:** If the IP configuration is assigned by the DHCP server, you can use the MAC address of the CMM network interface to find out what IP address is assigned.

To configure the CMM Ethernet ports, complete the following steps:

Step 1. Connect your system to the CMM command-line interface (see "Starting the command-line interface" on page 17 for more information).

Step 2. Configure the remote management and console (Ethernet) port (eth0), using the CMM CLI `ifconfig` command (see "ifconfig command" on page 174 for information about command use).

**Notes:**

- The internal Ethernet management port on each I/O module provides for communication with the CMM. You configure this port by configuring the IP address for the I/O module by using the web interface or the CMM CLI `ifconfig` command (see "ifconfig command" on page 174 for information about command use). See the documentation that comes with each I/O module for information and instructions. Some types of I/O modules, such as the pass-thru module, have no management port. See the documentation that comes with each I/O module to determine what else you must configure for the I/O module.
- For I/O-module communication with a remote management station, such as the optional Lenovo XClarity Administrator or Flex System Manager management node, through the CMM external Ethernet (remote management and console) port, the I/O-module internal network interface and the CMM internal and external interfaces must be on the same subnet.

- To communicate with the compute nodes for functions such as deploying an operating system or application program, you also must configure at least one external (in-band) port on an Ethernet I/O module.

## Serial over LAN

You can start an SOL session to any compute node that supports SOL.

Serial over LAN (SOL) provides a means to manage compute nodes remotely by using the CMM command-line interface (CLI) over a serial, Telnet, or Secure Shell (SSH) connection. SOL is required to manage compute nodes that do not have keyboard/video/mouse (KVM) support.

SOL provides console redirection for both the compute node firmware and operating system. The SOL feature redirects compute node serial-connection data over a LAN without the need for special cabling. The SOL connection enables compute nodes to be managed from any remote location with network access. SOL has the following advantages:

- Remote administration without keyboard, video, or mouse (headless servers)
- Reduced cabling and no need for a serial concentrator
- Standard Telnet interface that eliminates the need for special client software

The Lenovo Flex SystemCMM command-line interfaces provide access to the text-console command prompt on each compute node through an SOL connection, enabling the compute nodes to be managed from a remote location.

You access the compute node Integrated Management Module (IMM) CLI using a CMM SOL session (see "Starting an SOL session" on page 28). If no user accounts have been manually set up for the IMM of a compute node, connection to that IMM must be done using the current CMM user ID and password. In order for an IMM to communicate with the compute node Advanced Settings Utility (ASU) and UpdateXpress System Pack Installer (UXSPI) programs, a local user account must be set up for the compute node IMM. This local account is not included in an IMM configuration backup. For information about using the compute node IMM interface, see the compute node or IMM documentation.

**Note:** You can access the compute node IMM web interface using a CMM web interface remote console session (see "Starting a remote compute node session," in the *Lenovo Chassis Management Module 2 User's Guide*).

If security is a concern, use Secure Shell (SSH) sessions or connections that are made through the serial-management connector on the CMM to establish secure Telnet command-line interface sessions with the CMM before you start an SOL console redirect session with a compute node.

## Starting an SOL session

After you start a Telnet, serial, or SSH session to the Lenovo Flex SystemCMM, you can start an SOL session to any individual compute node that supports SOL.

**Note:** Serial over LAN (SOL) must be enabled for both the Lenovo Flex System chassis and the compute node before you can start an SOL session with the compute node. See "sol command" on page 319 for information about setting up and enabling SOL.

Because you can start up to 20 separate Telnet, serial, or SSH sessions to the Lenovo Flex SystemCMM, simultaneous SOL sessions can be active for each compute node in the Lenovo Flex System chassis.

Start an SOL session by using the `console` command (see "console command" on page 107 for information), from the command line, indicating the target compute node. For example, to start an SOL connection to the compute node in node bay 6, type

**console -T system:blade[6]**

**Note:** A node assembly that occupies more than one node bay is identified by the lowest bay number that it occupies.

After an SOL session is started, all commands are sent to the compute node that is specified by the `console` command until the SOL session is ended, regardless of the persistent command target that was in effect before the SOL session.

See "sol command" on page 319 for information about configuring a compute node for SOL. See your operating-system documentation for information about SOL commands that you can enter by using the command-line interface.

## Ending an SOL session

To end an SOL session, press Esc followed by an opening parenthesis.

When the SOL session ends, the command-line interface returns to the persistent command target that was in effect before the SOL session. If you want to end the Telnet or SSH command-line session, type `exit`.

**Note:** Exiting an SOL session does not stop the flow of serial data.

## Specifying a URL for file transfer

Some CLI commands require specification of a URL when transferring a file to or from the CMM.

**Note:** When the CMM is set to "Secure" security mode, only secure file transfer methods, such as HTTPS and SFTP, can be used for tasks involving file transfer when the CMM is acting as a server. Unsecure file transfer protocols, such as HTTP, FTP, and TFTP, are disabled when the CMM is acting as a server when the security mode is set to "Secure". Unsecure file transfer protocols remain available for a CMM acting as a client for all commands when the security mode is set to "Secure".

The CMM supports multiple server protocols for file transfer. The URLs for all protocols follow the same basic format:

***protocol*://*user*:*password*;fingerprint=*hostkey*@*hostname*:*port*/*path*/*filename***

Where:

- *protocol*: Protocol to use for server connection (tftp, ftp, http, https, or sftp).
- *user*: Optional user name for server connection.
- *password*: Optional password for user authentication during server connection. The password can be used only when a user is specified.
- *hostkey*: Optional host key used to authenticate an encryption key file. This host key can be used only when a user is specified. The fingerprint and hostkey are optional during secure operation.
- *hostname*: Server hostname.
- *port*: Optional server port to use for file transfer. The server port must be specified, if not using the default server port.
- *path*: Path to the file on the server.
- *filename*: File name of file being transferred.

**Examples:**

- To restore the CMM configuration from an image previously saved to an unencrypted file named cmm1. cfg and a passphrase of 'backuplock' in the temp directory on a TFTP server with an IP address of 9.37.177.215, while CMM 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type
**read -u tftp://9.37.177.215/temp/cmm1.cfg -p "backuplock"**
- To update the CMM firmware from a HTTP server and reboot the CMM in CMM bay 2 after a successful update, type the following command at the `system:>` prompt. For this example, the IP address of the HTTP server is 10.12.100.109 and the firmware file containing the update is named cmefs.uxp, that is in the flash sub-directory on the server. The verbose mode and reboot flag are also specified.
**update -u http://10.12.100.109/flash/cmefs.uxp -T mm[2] -v -r**
- To save the CMM configuration to a unencrypted file named cmm1.cfg and a passphrase of 'backuplock' in the temp directory on a TFTP server with an IP address of 9.37.177.215, while CMM 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type
**write -u tftp://9.37.177.215/temp/cmm1.cfg -p "backuplock"**
- To download a key with an index of 1, of type openssh, for the user named test, from an SFTP server with a host name of 10.40.1.15, where the key is in the /home/user directory, with a file name of file.ext, while CMM 2 is set as the persistent command environment, at the `system:mm[2]>` prompt, type the following command. The server is being accessed using a user name of user, a password of pass, and an optional fingerprint of sh-dss:14-25-f1-76-75-32-06-8b-ba-a6-e7-b8-23-44-40-34.
**users -n test -dnld -ki 1 -kf openssh -u sftp://user:pass;fingerprint=ssh-dss:14-25-f1-76-75-32-06-8b-ba-a6-e7-b8-23-44-40-34@10.40.1.15/home/user/file.ext**

  **Notes:** The URL for this downloaded file includes the following parameters:

  - Protocol type: `sftp`.
  - User name and password for server connection: `user` and `pass`.
  - Fingerprint preamble: `ssh-dss`. The fingerprint parameter must include a fingerprint preamble.
  - Fingerprint parameter: `c1:df:07:c4:e5:6a:7f:ce:47:a1:de:df:84:51:5f:bf`.
  - Server hostname: `10.40.1.15`.
  - Path on server: `/home/user`.
  - File name: `file.ext`.
- To download a key with an index of 1, of type openssh, for the user named test, from an SFTP server with a host name of 10.40.1.15, where the key is in the /home/user directory, with a file name of file.ext, while CMM 2 is set as the persistent command environment, at the `system:mm[2]>` prompt, type the following command. The server is being accessed using a user name of user, a password of pass; no optional fingerprint is specified in this example.
**users -n test -dnld -ki 1 -kf openssh -u sftp://user:pass@10.40.1.15/home/user/file.ext**

  **Notes:** The URL for this downloaded file includes the following parameters:

  - Protocol type: `sftp`.
  - User name and password for server connection: `user` and `pass`.
  - Server hostname: `10.40.1.15`.
  - Path on server: `/home/user`.
  - File name: `file.ext`.

## External authentication of certificates

Certificates are used to establish secure, trusted connections to the CMM and from the CMM to other servers.

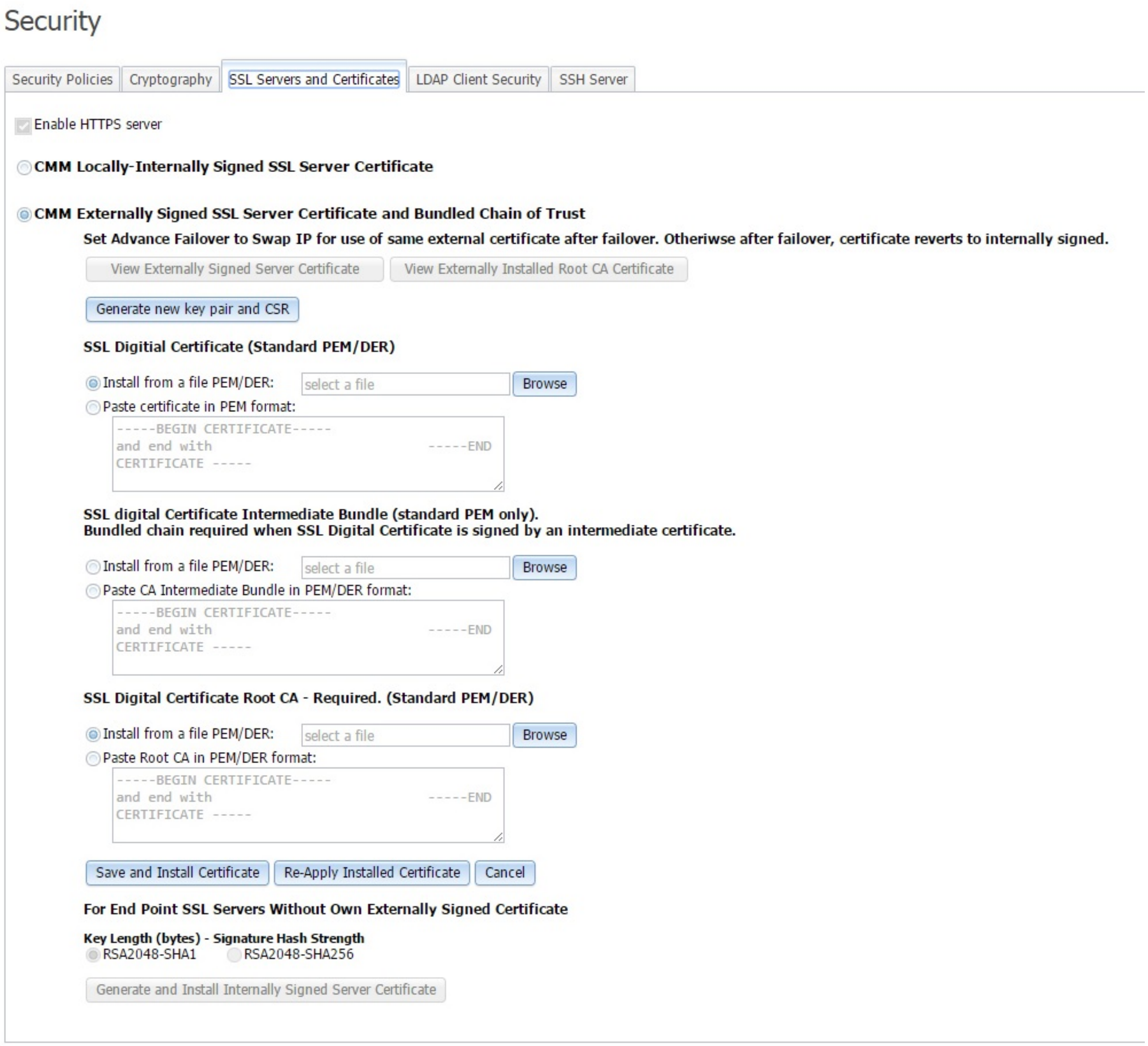
For an application initiating a connection to trust the server that it is connecting to, it must have in its trust store a copy of either the server certificate or the certificate of the Certificate Authority (CA) that signed the server certificate. The CMM has a CA that signs certificates for the LDAP, HTTPS, and CIM servers of all systems management processors in a Flex System chassis. Some compute nodes, such as the x240 M5 compute node, can also create certificates that can be imported by the CMM. See the Integrated Management Module (IMM) documentation for your compute node for information and instructions.

You can create trust between your web browser and the HTTPS servers on the management processors in the chassis by importing the CA certificate into your web browser. Additionally, when you work with an external LDAP server, you can use the CMM web interface or CLI to configure either non-mutual (server only) or mutual certificate authentication.

The CA certificate in each Lenovo Flex System chassis is unique. You download CA certificates through the primary CMM in each chassis using the CMM web interface or CLI.

- In the CMM web interface, click **Mgt Module Management** > **Security** > **SSL Servers and Certificates** > **CMM Externally Signed SSL Server Certificate and Bundled Chain of Trust**. Select the certificate type and format, and click **Save and Install Certificate**.
- In the CLI, download the CA certificate into the CMM by using the `sslcfg -dnld` command (see “sslcfg command” on page 328 for additional information about command use).

The following illustration shows the certificate download window.


Security
Security Policies
Cryptography
SSL Servers and Certificates
LDAP Client Security
SSH Server
View Externally Signed Server Certificate
View Externally Installed Root CA Certificate
Generate new key pair and CSR
Browse
Save and Install Certificate
Re-Apply Installed Certificate
Cancel
Generate and Install Internally Signed Server Certificate

☑ Enable HTTPS server

○ **CMM Locally-Internally Signed SSL Server Certificate**

● **CMM Externally Signed SSL Server Certificate and Bundled Chain of Trust**

**Set Advance Failover to Swap IP for use of same external certificate after failover. Otheriwse after failover, certificate reverts to internally signed.**

**SSL Digitial Certificate (Standard PEM/DER)**

● Install from a file PEM/DER: select a file

○ Paste certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
and end with                                -----END
CERTIFICATE -----
```

**SSL digital Certificate Intermediate Bundle (standard PEM only).**
**Bundled chain required when SSL Digital Certificate is signed by an intermediate certificate.**

○ Install from a file PEM/DER: select a file

○ Paste CA Intermediate Bundle in PEM/DER format:

```
-----BEGIN CERTIFICATE-----
and end with                                -----END
CERTIFICATE -----
```

**SSL Digital Certificate Root CA - Required. (Standard PEM/DER)**

● Install from a file PEM/DER: select a file

○ Paste Root CA in PEM/DER format:

```
-----BEGIN CERTIFICATE-----
and end with                                -----END
CERTIFICATE -----
```

**For End Point SSL Servers Without Own Externally Signed Certificate**

**Key Length (bytes) - Signature Hash Strength**
● RSA2048-SHA1 ○ RSA2048-SHA256

After you download each CA certificate, you should import it into your web browser, so that the web browser will trust websites that have a certificate signed by the CA. If there are multiple users who will access the management processors in the Flex System chassis, you can share the CA certificates with the other users. You can share certificates via email or through any other file sharing mechanism. Each user that receives a CA certificate must also import it into their web browser. If your organization has a process for pushing trusted authority certificates to users, you can also use that process.

To import a CA certificate into your web browser, complete the following steps:

1. Go to the area in your web browser where you configure web browser options and settings.
2. Locate and select managing certificates. In some web browsers, this selection is in the **Content** page or in the **Encryption** page on the **Advanced** page.
3. If you have old certificates that are related to this chassis, you should remove, delete, or distrust them, especially if you are experiencing errors relating to certificates. Check all tabs in the certificate page and remove all certificates related to this chassis. The “Issued by” field, if displayed, will indicate the chassis ID and time that the certificate was issued, in the form “CA for *chassis_uuid*, *time_stamp*.” For browsers where certificates are grouped in a tree structure by organization name, you will find the certificates in the “Generated by Firmware” section.

4. Import the CA certificate as a root authority certificate (not as a server certificate, intermediate authority, or other software device). Importing the CA certificate in this way might require that you are on the **Authorities** page before clicking **Import** and that you select a particular trusted root certificate store from the import wizard. During the import process, when asked to select the file that you want to import, you might need to change the file type to “All Files” to see the file that you want to import. If you are asked why you want to trust the certificate, choose the option that trusts the CA for identifying websites. Select **OK** or **Close** in all the pages you opened. If you are importing the CA certificate from more than one chassis, repeat this step for the CA certificates from each chassis.
5. Close your web browser and re-open it to make sure that these changes take effect.

If you change a CA certificate, you must download the new certificate and import it into your web browser, Lenovo XClarity Administrator, the Certificate Trust Store of your Flex System Manager management software, into any Lenovo Systems Director servers that might be in your network, and into any external LDAP servers that might be configured for mutual authentication (see “Importing an LDAP certificate with mutual authentication” on page 34 for information and instructions). This applies for all activities that can change a CA certificate such as manual changes or resetting the CMM to defaults.

If your web browser advises you that a connection is untrusted or a security certificate is invalid, or has any other issue that indicates a certificate exception issue relating to a certificate exception, follow the process given above to download and import the CA certificate, making sure to clear all old certificates from the chassis on all tabs in the certificate pages. You can also try clearing the browser cache and follow other instructions that might be suggested by the documentation for your web browser. Since some certificate issues impact only certain web browsers, you might be able to correct the condition by switching to a different web browser.

## Importing an LDAP certificate with non-mutual authentication

To authenticate an LDAP server with the CMM, you must import either the certificate of the LDAP server or the certificate of the Certificate Authority (CA) which signed the LDAP server certificate. The process for importing either an LDAP server certificate or the certificate of the CA with non-mutual authentication is the same.

Import a certificate by using non-mutual external authentication when you only have to authenticate the LDAP server with the CMM. You can authenticate the LDAP server with the CMM using the CMM management interface.

**Note:** Certificates must be signed using SHA-1 hashes, SHA-2 hashes are not supported.

To import an LDAP certificate or a CA, by using non-mutual authentication, complete the following steps:

Step 1. Obtain the external LDAP certificate or CA and place it on the server that will be used to import it. Depending on your CMM configuration, supported server types can include TFTP, FTP, HTTP, HTTPS, and SFTP.

Step 2. Start a CMM management session:

- To start a CMM CLI session, see “Starting the command-line interface” on page 17 for instructions.

  **Note:** For the CLI, the `sslcfg` command must be targeted to the primary CMM. The following example assumes that the command environment has been set to the primary CMM through the `env` command (see “env command” on page 131 for information about command use). If the command environment has not been set to the primary CMM, you can direct the command to the primary CMM by using the `-T mm[p]` option, (see “Command targets” on page 6 for information).

Step 3. Import the external LDAP certificate or CA into the CMM:

- In the CLI, import the external LDAP certificate or CA into the CMM by using the `sslcfg` command (see “sslcfg command” on page 328 for additional information about command use):
  `sslcfg -tc1 import -u` *file_location_on_server*
  where:

  – `-tc1` indicates trusted certificate 1. `-tc2` or `-tc3` can also be used to specify trusted certificates 2 and 3.

  – *file_location_on_server* is a fully qualified location that specifies the server type, the IPv4 or IPv6 IP address of the server, and a valid file name of the certificate file, of up to 256 characters and containing any character except the percent sign ( % ) or double quotation mark ( " ). The forward slash ( / ) can be used only as part of the path name, not as part of the file name.

  **Note:** For information about how to specify a URL for file transfer, see “Specifying a URL for file transfer” on page 29.

## Importing an LDAP certificate with mutual authentication

Import certificates for mutual authentication when you need the external LDAP server to authenticate the CMM and the CMM to authenticate the external LDAP server.

There are two ways to establish mutual authentication between the CMM and an external LDAP server. When you use either method, you must also perform the steps for non-mutual authentication.

- Export the chassis Certificate Authority (CA) certificate and import it into the trust store for your external LDAP server. This allows mutual authentication between the LDAP server and all elements in the chassis that have their security configuration automatically provisioned.
- Export a certificate-signing request (CSR) from the CMM and have it signed by a Certificate Authority that the LDAP server already trusts. This method provides mutual authentication between only the CMM and the LDAP server.

### Mutual authentication using CA

To use the CMM certificate authority (CA) with an external LDAP server, you must import the CA certificate into the external LDAP server trust store. Up to three trusted certificates can be imported.

To establish mutual authentication using the CMM CLI, complete the following steps:

1. Import the external LDAP server certificate or the CA chain that signed it into the CMM as an LDAP trusted certificate, as described in “Importing an LDAP certificate with non-mutual authentication” on page 33.
2. Start a CMM CLI session (see “Starting the command-line interface” on page 17 for instructions).

   **Notes:**

   - The CMM does not support external LDAP servers that use the certificate authority SHA256 to sign their certificates
   - The `sslcfg` command must be targeted to the primary CMM. The following example assumes that the command environment has been set to the primary CMM through the `env` command (see “env command” on page 131 for information about command use). If the command environment has not been set to the primary CMM, you can direct the command to the primary CMM by using the `-T mm[p]` option (see “Command targets” on page 6 for information).
3. Make sure that secure LDAP is enabled by using the CMM CLI `sslcfg -client enabled` command. See “sslcfg command” on page 328 for additional information about command use.
4. Download the CMM CA to the specified server by using the CMM CLI `sslcfg` command. Depending on your CMM configuration, supported server types can include TFTP, FTP, HTTP, HTTPS, and SFTP. See “sslcfg command” on page 328 for additional information about command use.

**sslcfg -dnld ca -u *URL_of_location_to_put_file***
where *URL_of_location_to_put_file* is a fully qualified location that specifies the server type, the IPv4 or IPv6 IP address of the server, and a valid file name, of up to 256 characters and containing any character except the percent sign ( % ) or double quotation marks ( " ). The forward slash ( / ) can be used only as part of the path name, not as part of the file name.

**Note:** For information about how to specify a URL for file transfer, see “Specifying a URL for file transfer” on page 29.

5. Move the CA file from the server, where you downloaded it, to the external LDAP server.
6. When the CA file is on the external LDAP server, import it so that the LDAP server trusts the certificate from the CMM (see the documentation for your LDAP server for information and instructions).

## Mutual authentication of CSR

To establish mutual authentication between the CMM and an external LDAP server, have the CMM certificate-signing request (CSR) signed by an outside Certificate Authority (CA) using the CMM management interface.

To generate a CSR on the CMM and get it signed by using the CMM CLI, complete the following steps:

1. Start a CMM CLI session (see “Starting the command-line interface” on page 17 for instructions).

   **Note:** The `sslcfg` command must be targeted to the primary CMM. The following example assumes that the command environment has been set to the primary CMM through the `env` command (see “env command” on page 131 for information about command use). If the command environment has not been set to the primary CMM, you can direct the command to the primary CMM by using the `-T mm[p]` option (see “Command targets” on page 6 for information).
2. Generate the CSR on the CMM by using the CMM CLI `sslcfg` command (see “sslcfg command” on page 328 for additional information about command use):
   **sslcfg -gen csr -c "*country*" -sp "*state*" -cl "*city*" -on "*org*" -hn *hostname***
   The required options are as follows:

   - *country* is two-character alphabetic code for the country, in double quotation marks.
   - *state* is a state or province name of up to 60 characters in length, in double quotation marks.
   - *city* is a city or locality name of up to 50 characters in length, in double quotation marks.
   - *org* is an organization name of up to 60 characters in length, in double quotation marks.
   - *hostname* is a valid host name of up to 60 characters in length.

   **Note:** You can specify additional optional fields for the CSR, if needed (see “sslcfg command” on page 328 for additional information).
3. Download the CMM CSR to the specified server by using the CMM CLI `sslcfg` command. Depending on your CMM configuration, supported server types can include TFTP, FTP, HTTP, HTTPS, and SFTP. See “sslcfg command” on page 328 for additional information about command use.
   **sslcfg -dnld csr -u *URL_of_location_to_put_file***
   where *URL_of_location_to_put_file* is a fully qualified location that specifies the server type, the IPv4 or IPv6 IP address of the server, and a valid file name of up to 256 characters and containing any character except the percent sign ( % ), forward slash ( / ), or double quotation marks ( " ).

   **Note:** For information about how to specify a URL for file transfer, see “Specifying a URL for file transfer” on page 29.
4. Using the approved procedure for your organization, sign the CSR; then, place the signed certificate on a TFTP server for uploading.
5. Import the signed certificate to the CMM by using the CMM CLI `sslcfg` command (see “sslcfg command” on page 328 for additional information about command use):
   **sslcfg -upld -u *URL_of_certificate_location***
   where *URL_of_certificate_location* is a fully qualified location that specifies the IPv4 or IPv6 IP address of the server and a valid file name, of up to 256 characters and containing any character except the percent

sign ( % ) or double quotation marks ( " ). The forward slash ( / ) can be used only as part of the path name, not as part of the file name.

**Note:** For information about how to specify a URL for file transfer, see “Specifying a URL for file transfer” on page 29.

6. Make sure that the certificate or the certificate chain of the entity that signed the new CMM LDAP client certificate is imported into the LDAP server. This makes sure that the LDAP server trusts the certificate (see the documentation for your LDAP server for information and instructions).
7. Note that this procedure allows the external LDAP server to trust the CMM, but not any other management components in the Lenovo Flex System chassis. For the external LDAP server to trust other management components, such as IMMs, import the CA into the external LDAP server, following the steps in “Mutual authentication using CA” on page 34, or, if the chassis policy allows, export a CSR from each management component, get it signed, and import it back into the corresponding Lenovo Flex System chassis management component.

# Chapter 3. Command reference

Each command topic describes an Lenovo Flex SystemChassis Management Module 2 command-line interface command, providing information about its function, syntax, and usage, with examples.

Adding a `-h`, `-help`, or `?` option to a command displays syntax help for that command. For example, to display help for the environment command, type one of the following commands:

- `env -h`
- `env -help`
- `env ?`

You can target a command to a device other than the one that is set as the default by adding a `-T` option to a command. See "Command targets" on page 6 for information.

Commands are listed in alphabetic order.

## accesscontrol command

This command displays and configures user access policies based on IP/MAC.

User can configure to allow or deny user access based on their IP/MAC. The list associated with a policy can include maximum of 10 IPV4, 10 IPV6 and 10 MAC (30 in total) addresses. There are three policies available:

- White List : Only the IP/MAC addresses in the table are allowed to access.
- Black List : All IP/MAC addresses are allowed to access except those in the table, whose access is denied.
- No policies: All the other policies will be removed when selected.

Following is an example of access control command:

`accesscontrol -T` *mm[P]* -black `-start_d` *11/01/2016* `-start_h` *14:45:00* `-stop_d` *11/01/2016* `-stop_h` 15:22:00 `-i4` *172.20.25.195* `-mac` *34-40-B5-DF-71-32* `-i6` *9000::8000* `-enable`

**Notes:**

- User can set a timeframe for the policy to take place by entering starting and ending date. Otherwise, the newly selected policy takes effects immediately.
- The selected policy persists after system reboot, but will be erased after system downgrade when the system goes to a version lower than 1.3.0.
- To comply with security requirement for this feature, do not use advance failover with "Do not swap Management Module IP addresses" option.

| Function | What it does | Command | Target (see paths in ) |
|---|---|---|---|
| **No policies** | Disables access control and removes all the previously created rules. | `accesscontrol -off` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

| | | | |
|---|---|---|---|
| **Create white list** | Creates a white list of IPs/ MACs with permission to access the CMM.<br>• -i4/-i6/-mac: the IPV4/ IPV6/MAC addresses to be included in the white list.<br>• -i4_d/-i6_d/-mac_d: the IPV4/IPV6/MAC addresses to be removed from the white list.<br>**Note:** The list associated with a policy can include maximum of 10 IPV4, 10 IPV6 and 10 MAC (30 in total). | `accesscontrol -white -i4` *ip_v4* `-i6` *ip_v6* `-mac` *mac_addr* `-i4_d` *ip_v4* `-i6_d` *ip_v6* `-mac_d` *mac_addr* where<br>• *ip_v4* is one or more IPV4 addresses.<br>• *ip_v6* is one or more IPV6 addresses.<br>Accepted format: xx:xx: xx:xx:xx:xx:xx (Short IPV6 is accepted as well. Ex: xx::xx).<br>• *mac_addr* is one or more MAC addresses.<br>Accepted format: xx-xx-xx-xx-xx-xx. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Create black list** | Creates a black list of IPs/ MACs that will be denied acces sto the CMM.<br>• -i4/-i6/-mac: the IPV4/ IPV6/MAC addresses to be included in the black list.<br>• -i4_d/-i6_d/-mac_d: the IPV4/IPV6/MAC addresses to be removed from the black list.<br>**Note:** The list associated with a policy can include maximum of 10 IPV4, 10 IPV6 and 10 MAC (30 in total). | `accesscontrol -black -i4` *ip_v4* `-i6` *ip_v6* `-mac` *mac_addr* `-i4_d` *ip_v4* `-i6_d` *ip_v6* `-mac_d` *mac_addr* where<br>• *ip_v4* is one or more IPV4 addresses.<br>• *ip_v6* is one or more IPV6 addresses.<br>Accepted format: xx:xx: xx:xx:xx:xx:xx (Short IPV6 is accepted as well. Ex: xx::xx).<br>• *mac_addr* is one or more MAC addresses. Accepted format: xx-xx-xx-xx-xx-xx. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set starting time** | Sets a policy to start at an appointed time and date. | `accesscontrol -white/black -start_h` *time* `-start_d` *date*<br>where<br>• *time* is an exact time.<br>Accepted format: hh: mm:ss.<br>• *date* is a date.<br>Accepted format: mm/ dd/yyyy. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

| | | | |
|---|---|---|---|
| **Set ending time** | Sets a policy to stop at an appointed time and date. | `accesscontrol -white/ black -stop_h` *time* `-stop_d` *date*<br>where<br>• *time* is an exact time.<br>Accepted format: hh: mm:ss.<br>• *date* is a date.<br>Accepted format: mm/ dd/yyyy. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Enable a policy** | Enables a policy<br>**Note:** All set policies are disabled by default and will only become effective after being enabled. | `accesscontrol -black/ white -enable` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Disable a policy** | Disables a policy. | `accesscontrol -black/ white -disable` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

## accseccfg command

This command displays and configures user account security settings for the CMM, including password policies.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See “Common errors” on page 407 for a list of error messages that apply to all commands or “accseccfg command errors” on page 409 for a list of error messages that are specific to the accseccfg command.

Table 7. *accseccfg command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display account security settings** | Displays the user account security settings for the CMM. Returned values:<br>• Default security settings used (legacy, high, or custom)<br>• -alt: authentication logging timeout (in seconds)<br>• -am: user authentication method (local, ldap, localldap, or ldaplocal)<br>• -cp: complex password (on, off)<br>• -ct: CLI inactivity session timeout (in seconds)<br>• -dc: minimum number of different characters in the password (0 to 15) Note: only when -cp (complex password) is enabled.<br>• -de: default 'USERID' account password must be changed on next login (on, off)<br>• -ia: account inactivity alert time period (in days)<br>• -ici: log new login events from same user (on, off)<br>• -id: account inactivity disable time period (in days)<br>• -lf: maximum login failures (0 to 100)<br>• -lp: lockout period after maximum login failures (in minutes, 2880 maximum)<br>• -mls: maximum simultaneous user sessions<br>• -pc: password change on first access (on, off)<br>• -pe: password expiration time period (in days, 365 maximum)<br>• -pi: minimum password change interval (in hours)<br>• -rc: password reuse cycle (0 to 5)<br>• -wt: web inactivity session timeout (in minutes, none, or based on length of user session) | `accseccfg` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set account security defaults to legacy level** | Sets CMM account security to a predefined legacy set of default values. Legacy default values:<br>• -alt (authentication logging timeout): retains set value<br>• -am (user authentication method): retains set value<br>• -cp (complex password): off<br>• -ct (CLI inactivity session timeout): retains set value | `accseccfg -legacy`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 7. accseccfg command (continued)

| Function | What it does | Command | Target (see paths in "Command targets" on page 6) |
|---|---|---|---|
| | • -dc (minimum number of different password characters): 0<br>• -de (default account password change at next login): off<br>• -ia (account inactivity alert time period): 0<br>• -ici (log new login events from same user): retains set value<br>• -id (account inactivity disable time): 0<br>• -lf (maximum login failures): 20<br>• -lp (lockout period after maximum login failures): 2<br>• -mls (maximum simultaneous user sessions): retains set value<br>• -pc (password change on first access): off<br>• -pe (password expiration time): 0<br>• -pi (minimum password change interval): 0<br>• -rc (password reuse cycle): 0<br>• -wt (web inactivity session timeout): retains set value<br>**Notes:**<br>• Modifying any default values after setting the -legacy or -secure option changes the user account security setting indication to custom.<br>• Accounts can not be set to -legacy if the CMM chassis security level is set to secure by the "security command" on page 298.<br>• The user who is running the accseccfg -legacy command must have a password assigned.<br>• The -legacy option must be run alone and not in conjunction with any other accseccfg command options. | | |
| **Set account security defaults to high level** | Sets CMM account security to a predefined high set of default values. High default values are:<br>• -alt (authentication logging timeout): retains set value<br>• -am (user authentication method): retains set value<br>• -cp (complex password): on<br>• -ct (CLI inactivity session timeout): retains set value<br>• -dc (minimum number of different password characters): 2 | `accseccfg -high`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[x]`<br>where *x* is the primary CMM bay number. |

*Table 7. accseccfg command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | • -de (default account password change at next login): on<br>• -ia (account inactivity alert time period): 120<br>• -ici (log new login events from same user): retains set value<br>• -id (account inactivity disable time): 180<br>• -lf (maximum login failures): 20<br>• -lp (lockout period after maximum login failures): 60<br>• -pc (password change on first access): on<br>• -pe (password expiration time): 90<br>• -pi (minimum password change interval): 24<br>• -rc (password reuse cycle): 5<br>• -wt (web inactivity session timeout): retains set value<br>**Notes:**<br>• Modifying any default values after setting the -legacy or -secure option changes the user account security setting indication to custom.<br>• The user who is running the accseccfg -high command must have a password assigned.<br>• The -high option must be run alone and not in conjunction with any other accseccfg command options. | | |
| **Set authentication logging timeout** | Sets a custom value for the amount of time that the CMM will not log repeated authentication events (login or logout) by the same user.<br>**Note:** When managing the Lenovo Flex System chassis with a program that uses the Common Information Model (CIM) interface, such as the optional Lenovo XClarity Administrator, if the `accseccfg -alt` value is not set to `none`, the CIM interface uses a minimum authentication logging timeout of 3600 seconds whenever the `accseccfg -alt` value is set to less than 3600 seconds. Other CMM functions use the configured `accseccfg -alt` value. | `accseccfg -alt` *timeout*<br>where *timeout* is 0, 5, 30, 60, 300, 600, 1800, 3600, 43200, or 86400 seconds. If a value of `none` is entered, the initial and any repeated authentication events will never be logged.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 7. accseccfg command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set user authentication method** | Sets a custom value for CMM user authentication method.<br>**Important:** If the authentication method is set to `ldap` (ldap only), you might not be able to log in to the CMM if the LDAP server is unreachable or if login credentials are not correctly configured. | `accseccfg -am` *method*<br>where *method* is<br>• `local`<br>• `ldap`<br>• `localldap`<br>• `ldaplocal`<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Enable / disable complex password** | Enables or disables the complex password for CMM user authentication.<br>**Notes:**<br>• -cp must be on to set the CMM chassis security level to secure with the "security command" on page 298.<br>• -cp must be on to configure the -dc (minimum number of password character types) command option. Setting -cp to off will set -dc to 0.<br>• The user that is running the accseccfg -cp command must have a password assigned. | `accseccfg -cp` *state*<br>where *state* is `on` or `off` .<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set CLI inactivity timeout** | Sets the custom value for CMM CLI inactivity session timeout. | `accseccfg -ct` *timeout*<br>where *timeout* is from 0 to 4,294,967,295 seconds, inclusive.<br><br>This command can only be run by users who have the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 7. accseccfg command (continued)*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set minimum number of different characters for password** | Sets custom value for the minimum number of different characters to be used in a CMM password.<br>**Note:**<br>• The minimum number of different characters applies only when complex passwords are enabled (-cp on). Setting -cp to off will set -dc to 0.<br>• The -rc command option must be non-zero to configure the minimum number of password character types. Setting -rc to zero will set -dc to 0.<br>• If a -dc value is not set when setting -rc command option to a non-zero value, -dc will be set to a default value of 2. | `accseccfg -dc` *number*<br>where *number* is from 0 to 15, inclusive.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Enable / disable default administration password expiration** | Enables or disables the default administration password expiration for the CMM. If enabled, the manufacturing default 'USERID' account password must be changed at the next login.<br>**Note:** -de must be on to set the CMM chassis security level to secure with the "security command" on page 298. | `accseccfg -de` *state*<br>where *state* is `on` or `off` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set account inactivity alert time** | Sets custom value for CMM account inactivity alert time.<br>**Note:** The accseccfg -ia value must be less than the accseccfg -id value. | `accseccfg -ia` *time*<br>where *time* is from 0 to 365 days, inclusive.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 7. accseccfg command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set state for logging of login events from same IP address** | Enables or disables logging of new login events from the same user from the same IP address.<br>**Notes:**<br>• This value applies only if the value set by the `-alt` command option is set to something other than 0 or none.<br>• When managing the Lenovo Flex System chassis with a program that uses the Common Information Model (CIM) interface, such as the optional Lenovo XClarity Administrator, login event logging is treated as disabled by the CIM interface, regardless of the `accseccfg -ici` setting. Other CMM functions use the configured `accseccfg -ici` value. | `accseccfg -ici` *state*<br>where *state* is `on` or `off` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set account inactivity disable time** | Sets the custom value for CMM account inactivity disable time.<br>**Note:** The accseccfg -id value must be greater than the accseccfg -ia value. | `accseccfg -id` *time*<br>where *time* is from 0 to 365 days, inclusive.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set maximum number of login failures** | Sets the custom value for the maximum number of login failures before the CMM locks out a user. | `accseccfg -lf` *number*<br>where *number* is from 0 to 100, inclusive.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 7. accseccfg command (continued)*

| Function | What it does | Command | **Target** *(see paths in "*Command targets*" on page 6)* |
|---|---|---|---|
| **Set lockout period** | Sets the custom value for CMM account lockout period, used when the maximum number of login failures is exceeded. | `accseccfg -lp` *time*<br>where *time* is from 0 to 2880 minutes, inclusive.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set maximum LDAP sessions for user** | Sets the custom value for the maximum number of simultaneous login sessions allowed for a single LDAP user | `accseccfg -mls` *max_sessions*<br>where *max_sessions* is from 0 to 20, inclusive.<br>This command can only be run by users who have the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Enable / disable password change at first login** | Enables or disables the mandatory password change at first CMM login.<br>When on, new users must change their password the first time they log in. If a user password is changed by a system administrator, this user must change their password the next time they log in.<br>**Notes:**<br>• `accseccfg -pc` is set to on automatically when `accseccfg` is set to `-high`<br>• `accseccfg -pc` must be on to set the CMM chassis security level to secure with the "security command" on page 298. | `accseccfg -pc` *state*<br>where *state* is `on` or `off` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 7. accseccfg command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set password expiration time** | Sets custom value for the CMM password expiration time. | `accseccfg -pe` *time*<br>where *time* is from 0 to 365 days, inclusive.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set password minimum change interval** | Sets custom value for the minimum amount of time between CMM password changes.<br>**Note:** If the minimum password change interval is greater than 0, it must be less than password expiration period. | `accseccfg -pi` *time*<br>where *time* is from 0 to 1440 hours, inclusive, and less than password expiration period when that period is greater than 0.<br>This command can only be run by users who have the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 7. accseccfg command (continued)*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set password reuse cycle** | Sets custom value for the CMM password reuse cycle. This setting determines how many times a password must be changed before being reused.<br>**Note:**<br>• -rc must be non-zero to configure the -dc (minimum number of password character types) command option. Setting -rc to zero will set -dc to 0.<br>• If a -dc value is not set when setting -rc command option to a non-zero value, -dc will be set to a default value of 2. | `accseccfg -rc` *number_ reuses*<br>where *number_reuses* is from 0 to 5, inclusive.<br><br>This command can only be run by users who have the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set web interface inactivity timeout** | Sets custom value for CMM web interface inactivity session timeout. | `accseccfg -wt` *timeout*<br>where *timeout* is 1, 5, 10, 15, or 20 minutes, `none` (no timeout), or `user` (user picks timeout each time they log in to the web interface).<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

**Example:**

To set CMM account security to use the legacy level defaults, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
accseccfg -legacy -T mm[p]
```

To display the account security settings for the CMM, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
accseccfg -T mm[p]
```

To disable the authentication logging timeout for the CMM, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
accseccfg -alt none -T mm[p]
```

The following example shows the information that is returned from these commands:

```
system> accseccfg -legacy -T mm[p]
OK
system> accseccfg -T mm[p]
```

```
-legacy
-alt 300
-am local
-cp off
-ct 0
-dc 0
-de off
-ia 0
-ici off
-id 0
-lf 20
-lp 2
-mls 0
-pc off
-pe 0
-pi 0
-rc 0
-wt user
system> accseccfg -alt none -T mm[p]
OK
system>
```

## advfailover command

This command displays and configures the advanced failover settings for the CMM.

**Notes:**

- If a Lenovo Flex System chassis is set up for redundant CMM operation and both CMMs experience an unrecoverable failure, the chassis will attempt to switch control between the CMMs indefinitely. If this condition occurs, replace one CMM to return the chassis to operation or replace both CMMs to return the chassis to redundant operation. Depending on how each CMM failed, you might need to configure the replacement CMM or restore its configuration from a backup, if one is available. A failure of both CMMs might be an indication of other problems with the Lenovo Flex System chassis; make sure that the chassis is operating properly before replacing either CMM. See Troubleshooting chassis for information about diagnosing problems with a Lenovo Flex System chassis.
- For more information about CMM redundancy, see "Preparing for CMM redundancy" in the *Lenovo Flex System Chassis Management Module 2 Installation Guide*.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See “Common errors” on page 407 for a list of error messages that apply to all commands or “advfailover command errors” on page 411 for a list of error messages that are specific to the advfailover command.

*Table 8. advfailover command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display CMM advanced failover settings** | Displays the advanced failover settings for the CMM. Possible return values are:<br>• off - disable network interface for the standby CMM<br>• swap - enable the standby CMM network interface and swap IP addresses between the two CMMs during failover<br>• noswap - enable the standby CMM network interface and do not swap IP addresses between the two CMMs during failover<br>**Note:** When advanced failover is set to off, a CMM failover can be forced using the `reset -f` command (see "reset command" on page 289 for information). | `advfailover` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Disable network interface for standby CMM** | Disables the network interface for the standby CMM, preventing failover.<br>**Note:** When advanced failover is set to off, a CMM failover can be forced using the `reset -f` command (see "reset command" on page 289 for information). | `advfailover -ip off`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 8. advfailover command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Enable network interface and allow IP address swap during failover** | Enables the network interface for the standby CMM and allows the IP addresses to swap between the two CMMs during failover.<br>**Notes:**<br>• The `-ip swap` command option can not be run if only one CMM is installed in the chassis.<br>• If you enable IP address swapping during failover with both CMMs set to the same static IP address, you must disable DHCP (see "ifconfig command" on page 174 for information). | `advfailover -ip swap`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Enable network interface and prevent IP address swap during failover** | Enables the network interface for the standby CMM and prevents the IP addresses from swapping between the two CMMs during failover.<br>**Note:** The `-ip noswap` command option can not be run if only one CMM is installed in the chassis. | `advfailover -ip noswap`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

**Example:**

To disable the network interface for the standby CMM, while the primary CMM in bay 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
advfailover -ip off
```

To display the CMM advanced failover setting, while the primary CMM in bay 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
advfailover
```

The following example shows the information that is returned from these two commands:

```
system:mm[1]> advfailover -ip off
OK
system:mm[1]> advfailover
-ip off
system:mm[1]>
```

## airfilter command

This command sets the interval for air filter change notifications.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "airfilter command errors" on page 411 for a list of error messages that are specific to the airfilter command.

*Table 9. airfilter (set notification interval) command*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display air filter change notification interval** | Displays the frequency of the chassis air filter reminder. | `airfilter` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set air filter change notification interval** | Configures the frequency of the chassis air filter reminder.<br>**Note:** The 1 month replacement interval is recommended for environments with a high amount of dust. Replacement every 3 months is recommended for environments with medium amounts of dust. Replacement every 6 months is recommended for environments with low amounts of dust. | `airfilter -freq` *frequency*<br>where *frequency* is the interval, in months, between reminders to change the chassis air filter. Valid values are 0, 1, 3, and 6.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>• Chassis log management<br>• Chassis administration<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

**Example:** To view the current air filter notification interval, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

`airfilter -T mm[p]`

To set the air filter notification interval to three months, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

`airfilter -T mm[p] -freq 3`

The following example shows the information that is returned when these commands are entered:

```
system> airfilter -T mm[p]
-freq 1
system> airfilter -T mm[p] -freq 3
OK
system>
```

## alarm command

This command acknowledges or unacknowledges alarms, clears alarms, or creates custom alarms for the specified command target.

**Notes:**

- The alarm command applies only to CMMs installed in a Lenovo Flex System Carrier-Grade chassis.
- All alarm commands are processed at the chassis (`system` target) level. Specifying a command target (`-T` *target_name*) is optional: alarm commands issued to any command target will be accepted and processed.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "alarm command errors" on page 411 for a list of error messages that are specific to the alarm command.

Table 10. alarm command

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Acknowledge alarm** | Acknowledge the specified alarm ID for the command target.<br>**Note:** View alarms and their IDs using the "health command" on page 164. | `alarm -ack -i` *value*<br>where *value* is the 8-digit hexadecimal alarm ID shown by the `health` command.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration (for CMM, power supply, or fan module)<br>• Blade configuration (for compute node)<br>• I/O module configuration (for I/O module)<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system`<br>**Note:** Specifying a command target is optional. All alarm commands are processed at the chassis (`system` target) level. |
| **Clear alarm** | Clear the specified alarm ID for the command target.<br>**Note:** View alarms and their IDs using the "health command" on page 164. | `alarm -clear -i` *value*<br>where *value* is the 8-digit hexadecimal alarm ID shown by the `health` command.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration (for CMM, power supply, or fan module)<br>• Blade configuration (for compute node)<br>• I/O module configuration (for I/O module)<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system`<br>**Note:** Specifying a command target is optional. All alarm commands are processed at the chassis (`system` target) level. |

*Table 10. alarm command (continued)*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Unacknowledge alarm** | Unacknowledge the specified alarm ID for the command target.<br>**Note:** View alarms and their IDs using the "health command" on page 164. | `alarm -unack -i` *value*<br>where *value* is the 8-digit hexadecimal alarm ID shown by the `health` command.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration (for CMM, power supply, or fan module)<br>• Blade configuration (for compute node)<br>• I/O module configuration (for I/O module)<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system`<br>**Note:** Specifying a command target is optional. All alarm commands are processed at the chassis (`system` target) level. |
| **Create alarm** | Creates an alarm request for the specified target, including an alarm severity level and description. | `alarm -create -s` *level* `-p "` *desc* `"`<br>where<br>• *level* is the severity level:<br>– `CRT` (critical)<br>– `MJR` (major)<br>– `MNR` (minor)<br>• *desc* is a quote-delimited description of the alarm up to 63 characters in length.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration (for CMM, power supply, or fan module)<br>• Blade configuration (for compute node)<br>• I/O module configuration (for I/O module)<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system`<br>**Note:** Specifying a command target is optional. All alarm commands are processed at the chassis (`system` target) level. |

**Example:** To acknowledge a power alarm with an ID of 00000450 for the power supply in bay 2, while the Lenovo Flex System Enterprise Chassis is set as the persistent command environment, at the `system>` prompt, type
`alarm -ack -i 00000450`

The following example shows the information that is returned from this command.

```
system> alarm -ack -i 00000450
OK
system>
```

## alertcfg command

This command displays and configures the global remote alert settings for the CMM.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "alertcfg command errors" on page 412 for a list of error messages that are specific to the alertcfg command.

*Table 11. alertcfg command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display global remote alert settings** | Displays the global remote alert settings for the CMM. | `alertcfg` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set remote alert retry delay interval** | Sets the remote alert retry delay interval. | `alertcfg -dr` *delay*`-rl` *limit*<br>where *delay* is from 0.5 minutes to 4.0 minutes, inclusive, in 0.5 minute increments. If you enter a value less than 0.5 minute, the retry interval will be set to 0.5 minute. If you enter a value greater than 4.0 minutes, the retry interval will be set to 4.0 minutes.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 11. alertcfg command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Include / exclude service information with email alerts** | Enables or disables inclusion of service information with email alerts. | `alertcfg -si` *state*<br>where *state* is `enabled` or `disabled` .<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See “Commands and user authority” on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set remote alert retry limit** | Sets the maximum number of times the system will attempt to send a remote alert, if previous attempts were unsuccessful. | `alertcfg -rl` *value*<br>where *value* is from 0 to 8, inclusive. If you enter a value of 0, no retries will be attempted. If you enter a value greater than 8, an error will be displayed.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See “Commands and user authority” on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

**Example:** To view the remote alert configuration, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type
`alertcfg -T mm[p]`

To set the retry interval to 3.5 minutes, include service information in the alert, and set the remote alert retry limit to 7, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type
`alertcfg -dr 3.5 -si enabled -rl 7 -T mm[p]`

The following example shows the information that is returned from these commands:

```
system> alertcfg -T mm[p]
-dr 2.0
-si disabled
-rl 6
system> alertcfg -dr 3.5 -si enabled -rl 7 -T mm[p]
OK
system> alertcfg -T mm[p]
-dr 3.5
-si enabled
```

```
-rl 7
system>
```

## alertentries command

This command manages the recipients of alerts generated by the primary CMM.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "alertentries command errors" on page 412 for a list of error messages that are specific to the alertentries command.

*Table 12. alertentries command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display alert properties for all recipients** | Displays alert properties for all CMM alert recipients. Returned values for each alert recipient are:<br>• recipient name<br>• notification method (Email over LAN/Systems Director comp./SNMP over LAN)<br>• type of alerts received (Receives critical alerts only/Receives all alerts/ Disabled) | `alertentries` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Display alert properties for alert recipients** | Displays alert properties for the specified CMM alert recipient profile. Returned values are:<br>• -status *alert_recipient_status* (on/off)<br>• -n *alert_recipient_name*<br>• -f *alert_type* (critical/ none)<br>• -t *notification_method* (email/director/snmp)<br>• -e *email_address* (used for email notifications) | `alertentries` -*recip_number*<br>where *recip_number* is a number from 1 to 12 that corresponds to the recipient number assigned in the "Display alert properties for all recipients" list. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 12. alertentries command (continued)*

| Function | What it does | Command | **Target** *(see paths in "*Command targets*" on page 6)* |
|---|---|---|---|
| **Delete alert recipient** | Delete the specified alert recipient. | `alertentries` *-recip_number* `-del`<br>where *recip_number* is a number from 1 to 12 that corresponds to the recipient number assigned in the "Display alert properties for all recipients" list. It is possible to delete an empty alert recipient.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>• Chassis log management<br>• Chassis administration<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Create alert recipient** | Create the specified alert recipient.<br>All fields must be specified when creating an alert recipient. | `alertentries` *-recip_number* `-n` *recip_name* -status *alert_status* `-f` *filter_type* `-t` *notification_method* -e *email_addr*<br>where:<br>• *recip_number* is a number from 1 to 12 that corresponds to an unused recipient number in the "Display alert properties for all recipients" list.<br>• *recip_name* is a alphanumeric string up to 31 characters in length containing any character, including spaces, except for angle brackets ( < and > ). If the string includes spaces it must be enclosed in double-quotes.<br>• *alert_status* is `on` or `off` for receipt of alerts.<br>• *filter_type* filters the alert types received: `critical` (receive critical alerts only) or `none` (receive all alerts).<br>• *notification_method* is `email` or `snmp` .<br>– For `email` , you must specify an email address (-e argument).<br>– If `snmp` is selected, the -e argument is not needed.<br>• *email_addr* is a valid email address string up to 63 characters in length.<br>*(continued on next page)* | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 12. alertentries command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | | This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>• Chassis log management<br>• Chassis administration<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | |
| **Set alert recipient name** | Sets a name for the specified alert recipient. | `alertentries` -*recip_number* `-n` *recip_name*<br>where:<br>• *recip_number* is a number from 1 to 12 that corresponds to the recipient number assigned in the "Display alert properties for all recipients" list.<br>• *recip_name* is a alphanumeric string up to 31 characters in length that can include any character, including spaces, except for angle brackets ( < and > ). If the name includes spaces, it must be enclosed in double-quotes.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>• Chassis log management<br>• Chassis administration<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 12. alertentries command (continued)*

| Function | What it does | Command | **Target** *(see paths in "*Command targets*" on page 6)* |
|---|---|---|---|
| **Set alert recipient status** | Sets status for the specified alert recipient. The status determines if a recipient will receive alarm notifications. | `alertentries` *-recip_number* `-status` *alert_status*<br>where:<br>• *recip_number* is a number from 1 to 12 that corresponds to the recipient number assigned in the "Display alert properties for all recipients" list.<br>• *alert_status* is on or off.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>• Chassis log management<br>• Chassis administration<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set alert types received** | Filters the types of alert that are received by the specified alert recipient. | `alertentries` *-recip_number* `-f` *filter_type*<br>where:<br>• *recip_number* is a number from 1 to 12 that corresponds to the recipient number assigned in the "Display alert properties for all recipients" list.<br>• *alert_type* filters the alert types received: `critical` (receive critical alerts only) or `none` (receive all alerts).<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>• Chassis log management<br>• Chassis administration<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 12. alertentries command (continued)*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set alert notification method** | Sets the alert notification method for the specified alert recipient. | `alertentries` *-recip_number* `-t` *notification_method*<br>where:<br>• *recip_number* is a number from 1 to 12 that corresponds to the recipient number assigned in the "Display alert properties for all recipients" list.<br>• *notification_method* is<br>– `email`<br>– `snmp`<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>• Chassis log management<br>• Chassis administration<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set alert recipient email address** | Sets the email address for the specified alert recipient. This email address is used to send alerts to the recipient via email.<br>The email address can be set only if the alert notification method (-t option) is set to email. The -t and -e options can be combined within the same command. | `alertentries` *-recip_number* `-e` *email_addr*<br>where:<br>• *recip_number* is a number from 1 to 12 that corresponds to the recipient number assigned in the "Display alert properties for all recipients" list.<br>• *email_addr* is a valid email address string up to 63 characters in length.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>• Chassis log management<br>• Chassis administration<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Generate test alert** | Generates a test alert to verify correct alert response.<br>**Notes:**<br>• The `alertentries -test` command option must be used alone. | `alertentries -test`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>• Chassis log management<br>• Chassis administration | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 12. alertentries command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | - If autoftp is enabled, sending a test alert will cause the system to send out service data as well. | - Chassis configuration<br>See "Commands and user authority" on page 10 for additional information.<br><br>In some cases, your system configuration might also allow the command to be run by users who have one or more of the following command authorities:<br>- Chassis log management<br>- Chassis administration<br>- Blade administration<br>- Blade configuration<br>- Blade remote presence<br>- I/O module administration<br>- I/O module configuration<br><br>See "Commands and user authority" on page 10 for additional information. | |

**Example:** To view the configuration for alert recipient 1, while the primary CMM in bay 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type
`alertentries -1`

To configure alert recipient 2 to receive only critical alert notifications by email, while the primary CMM in bay 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type
`alertentries -2 -n test2 -status on -f critical -t email -e test2@lenovo.com`

To configure alert recipient 4 to receive all alert notifications through SNMP, while the primary CMM in bay 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type
`alertentries -4 -n test4 -status on -f none -t snmp`

The following example shows the information that is returned from these commands:

```
system:mm[1]> alertentries -1
-status on
-n test1
-f critical
-t email
-e test1@lenovo.com
system:mm[1]> alertentries -2 -n test2 -status on -f critical -t email
-e test2@us.lenovo.com
OK
system:mm[1]> alertentries -4 -n test4 -status on -f none -t snmp
OK
system:mm[1]>
```

## autoftp command

This command displays and configures the automated FTP/TFTP/SFTP problem report settings for the CMM.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "autoftp command errors" on page 413 for a list of error messages that are specific to the autoftp command.

Table 13. autoftp command

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display call-home settings for autoftp call home** | Displays the Automated FTP/TFTP/SFTP Problem Report settings that allow the CMM to automatically put service data onto a specified server when a call home event is detected. | `autoftp` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Configure call-home settings for autoftp call home** | Configures the Automated FTP/TFTP/SFTP Problem Report settings that allow the CMM to automatically put service data onto a specified server when a call home event is detected.<br>**Note:** The system will wait five days before sending duplicate events if they are left unacknowledged in the activity log. | `autoftp -m` *mode* `-i` *ip_address* `-p` *port* `-u` *"user_name"* `-pw` *"password"*<br>where:<br>• *mode* is one of the following automated problem reporting modes:<br>– `ftp`<br>– `tftp`<br>– `sftp`<br>– `disabled`<br>• *ip_address* is the IP address of the FTP, TFTP, or SFTP server<br>• *port* is the FTP, TFTP, or SFTP transmission port, a number from 1 to 65535, inclusive. If you enter a value outside this range, an error message will be displayed.<br>• *"user_name"* is the quote-delimited FTP or SFTP User Name for automated problem reporting (63 characters maximum).<br>• *"password"* is the quote-delimited FTP or SFTP password for automated problem reporting (63 characters maximum).<br>**Notes:**<br>• For FTP and SFTP, all fields must be set.<br>• For TFTP, only -i and -p are needed.<br>This command can only be run by users who have one or more of the following command authorities: | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 13. autoftp command (continued)*

| Function | What it does | Command | **Target** *(see paths in “Command targets” on page 6)* |
|---|---|---|---|
|  |  | • Supervisor<br>• Chassis configuration<br>See “Commands and user authority” on page 10 for additional information. |  |

**Example:**

To view the settings of the automated call-home message feature, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type
`autoftp -T mm[p]`

To configure the automated call-home message feature to report call-home events using TFTP to tftp.lenovo.com over transmission port 69, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type
`autoftp -m tftp -i tftp.lenovo.com -p 69 -T mm[p]`

The following example shows the information that is returned from these commands:

```
system> autoftp -T mm[p]
-m ftp
-i ftp.lenovo.com
-p 6
-u smlite
system> autoftp -m tftp -i tftp.lenovo.com -p 69 -T mm[p]
OK
system>
```

## baydata command

This command allows a user to set, assign, and display informational data assigned to the compute node bays.

**Note:** The data accessed by the `baydata` command belongs to the to the compute node bay and not to the device installed in the bay, so it is possible to direct the `baydata` command to a compute node bay that has no devices installed in it.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See “Common errors” on page 407 for a list of error messages that apply to all commands or “baydata command errors ” on page 414 for a list of error messages that are specific to the baydata command.

*Table 14. baydata command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display bay data for all compute nodes** | Displays compute node bay data for bay number, bay data status, and defined bay data for all bays. | `baydata` | Lenovo Flex System chassis:<br>`system` |
| **Display compute node bay data for a specific bay** | Displays the information assigned to the specified node bay.<br>**Note:** You must direct the `baydata` command to the correct compute node target, based on your specific system configuration. See the information about the `-b` *bay_num* argument in the Command column for instructions. | `baydata -b` *bay_num*<br>where *bay_num* :<br>• identifies the chassis compute node bay number, if the compute node is installed directly in the chassis (`system:blade[`*x*`]`). For example, a compute node in chassis compute node bay 1 would be identified as `baydata -b 1`.<br>• identifies both the chassis compute node bay number and the blade group subslot number, separated by a colon (:), if the compute node is part of a blade group (`system:bladegroup[`*x*`]:blade[`*y*`]`). For example, a compute node in subslot 2 of a blade group in chassis compute node bay 1 would be identified as `baydata -b 1:2`.<br>The bay number must be within the scope assigned to the user. Valid subslot numbers are 1 and 2.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system` |

*Table 14. baydata command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Clear bay data** | Clears the node bay definition strings for all compute nodes bays within the user's scope. | `baydata -clear`<br>The bay numbers must be within the scope assigned to the user.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system` |
| **Clear bay data for specific bay** | Clears the node bay definition strings for the specified node bay.<br>**Note:** You must direct the `baydata` command to the correct compute node target, based on your specific system configuration. See the information about the `-b` *bay_num* argument in the Command column for instructions. | `baydata -b` *bay_num* `-clear`<br>where *bay_num* :<br>• identifies the chassis compute node bay number, if the compute node is installed directly in the chassis (`system:blade[`*x*`]`). For example, a compute node in chassis compute node bay 1 would be identified as `baydata -b 1`.<br>• identifies both the chassis compute node bay number and the blade group subslot number, separated by a colon (:), if the compute node is part of a blade group (`system:bladegroup[`*x*`]:blade[`*y*`]`). For example, a compute node in subslot 2 of a blade group in chassis compute node bay 1 would be identified as `baydata -b 1:2`.<br>The bay number must be within the scope assigned to the user. Valid subslot numbers are 1 and 2.<br>This command can only be run by users who have one or more of the | Lenovo Flex System chassis:<br>`system` |

Table 14. baydata command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | | following command authorities:<br>• Supervisor<br>• Blade configuration<br>See "Commands and user authority" on page 10 for additional information. | |
| **Set bay data** | Sets node bay data for all compute nodes within the user's scope. This information can include: data about drivers or software, the Lenovo Flex System chassis shelf number and IP address, and whether the compute node is a master or member in a high-availability system.<br>**Note:** To apply changes to the BIOS/SMBIOS structure, power-off and power-on the compute node, restart the compute node, or remove and reinstall the compute node. | `baydata -data` "*data_ definition*"<br>where "*data definition*" is the ASCII string of up to 60 characters enclosed in double quotation marks - "data definition". The quotation marks are not stored.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system` |

Table 14. baydata command (continued)

| Function | What it does | Command | Target (see paths in "Command targets" on page 6) |
|---|---|---|---|
| **Set node bay data definition for specific compute node** | Sets node bay data for the specified compute node.<br>**Notes:**<br>• To apply changes to the BIOS/ SMBIOS structure, power-off and power-on the compute node, restart the compute node, or remove and reinstall the compute node.<br>• You must direct the `baydata` command to the correct compute node target, based on your specific system configuration. See the information about the `-b` *bay_num* argument in the Command column for instructions.<br>If the command is issued to a specific bay, data is written to that compute node if it is in the user's scope. | `baydata -b` *bay_num* `-data` "*data_definition*"<br>where:<br>• where "*data definition*" is the quote-delimited ASCII string of up to 60 characters<br>• where *bay_num* :<br>– identifies the chassis compute node bay number, if the compute node is installed directly in the chassis (`system: blade[`*x*`]`). For example, a compute node in chassis compute node bay 1 would be identified as `baydata -b 1`.<br>– identifies both the chassis compute node bay number and the blade group subslot number, separated by a colon (:), if the compute node is part of a blade group (`system: bladegroup[`*x*`]: blade [`*y*`]`). For example, a compute node in subslot 2 of a blade group in chassis compute node bay 1 would be identified as `baydata -b 1:2`.<br>The bay number must be within the scope assigned to the user. Valid subslot numbers are 1 and 2.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system` |

**Example:** To view the bay data for all compute nodes, while the CMM is set as the persistend command environment, at the `system>` prompt, type

```
baydata
```

The following example shows the information that is returned from this command:

```
system> baydata
Bay   Status             Definition
1     No blade present  baydata1
1:1   No blade present
1:2   No blade present
2     No blade present
2:1   No blade present
2:2   No blade present
3     Unsupported
3:1   BSMP
3:2   BSMP
4     BSMP
4:1   No blade present  baydata 4:1
4:2   No blade present
5     Unsupported
5:1   No blade present
5:2   No blade present
6     No blade present
6:1   No blade present
6:2   No blade present
7     Unsupported
7:1   Unsupported
7:2   Unsupported
8     No blade present
8:1   No blade present
8:2   No blade present
9     No blade present
9:1   No blade present
9:2   No blade present
10    No blade present
10:1  No blade present
10:2  No blade present
11    Unsupported
11:1  Unsupported
11:2  Unsupported
12    No blade present
12:1  No blade present
12:2  No blade present
13    No blade present
13:1  No blade present
13:2  No blade present
14    No blade present
14:1  No blade present
14:2  No blade present
system>
```

## bootmode command

This command sets and displays the boot mode settings for compute nodes installed in the Lenovo Flex System chassis that support this feature.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "bootmode command errors" on page 414 for a list of error messages that are specific to the bootmode command.

*Table 15. bootmode command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display compute node boot mode** | Displays the boot mode settings of the specified compute node.<br>**Note:** This command will execute only on compute nodes that support the bootmode feature. | `bootmode` | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |
| **Set compute node boot mode** | Sets the copy of firmware that the specified compute node will use to boot:<br>• Temporary: booting from the temporary copy is recommended since it typically contains the latest enhancements and fixes.<br>• Permanent: booting from the permanent copy should be used only when booting from the temporary copy is no longer possible.<br>Changes to the boot mode setting take effect after the next restart of the compute node.<br>**Note:** This command will execute only on compute nodes that support the bootmode feature. | `bootmode -p` *mode*<br>where *mode* is:<br>• `temp` for temporary firmware copy.<br>• `perm` for permanent firmware copy.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade configuration<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |

**Example:** To view the boot mode of the compute node in bay 2, while this compute node is set as the persistent command environment, at the `system:blade[2]>` prompt, type

```
bootmode
```

To set the boot mode of the compute node in bay 2 to permanent, while this compute node is set as the persistent command environment, at the `system:blade[2]>` prompt, type

```
bootmode -p perm
```

The following example shows the information that is returned from these commands:

```
system:blade[2]> bootmode
active: temporary
pending: Invalid boot mode type
system:blade[2]> bootmode -p perm
Set the blade boot mode to permanent succeeded.
The setting will become active after the next reboot of the blade.
system:blade[2]> bootmode
active: temporary
pending: permanent
system:blade[2]>
```

## bootseq command

This command sets and displays the boot sequence settings for compute nodes installed in the Lenovo Flex System chassis.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "bootseq command errors" on page 415 for a list of error messages that are specific to the bootseq command.

*Table 16. bootseq command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display compute node boot sequence** | Displays the boot sequence of the specified compute node. The command returns a list of all boot devices assigned to the command target, with their order and IDs, and a list of all available boot devices with their information. | `bootseq` | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |
| **Set boot sequence for compute node** | Sets the boot sequence of the specified compute node.<br>**Note:** The -seq option must be used exclusive of all other command options. | `bootseq -seq` *devicelist*<br>where *devicelist* has one or more of the boot device IDs specified, as a pipe-separated (\|) list in order of preference.<br>A boot sequence of up to five boot devices can be specified and it can be seen by running the `bootseq` command with no options. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |
| **Display information for boot device** | Displays settings for the specified boot device. | `bootseq -id` *ID*<br>where *ID* is the boot device ID of the boot device.<br>Valid boot device IDs can be seen by running the `bootseq` command with no options. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |

*Table 16. bootseq command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set IP address for boot device (IPv4)** | Sets IPv4 IP address information for specified boot device of the command target.<br>**Notes:**<br>- A boot device must be specified using the -id command option.<br>- Use the -i, -g, or -s options with no argument to clear the setting.<br>- The host address, net mask, and gateway address must all be specified.<br>- After IP address information is initially set, each option can be modified individually. | `bootseq -id` *device_id* `-i` *hostaddr* `-g` *netmask* `-s` *gateway*<br>where:<br>- *device_id* is a unique ID for the boot device.<br>- *hostaddr* is the boot device IPv4 host address.<br>- *netmask* is the boot device IPv4 netmask.<br>- *gateway* is the boot device IPv4 gateway address.<br>Valid boot device IDs can be seen by running the `bootseq` command with no options.<br>This command can only be run by users who have one or more of the following command authorities:<br>- Supervisor<br>- Blade configuration<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |
| **Clear IP address for boot device** | Clears IP address information for specified boot device of the command target.<br>**Notes:**<br>- A boot device must be specified using the -id command option.<br>- The IP address options are cleared by entering no arguments.<br>- The host address, net mask, and gateway address must all be cleared together. | `bootseq -id` *device_id* `-i -g -s`<br>where *device_id* is a unique ID for the boot device.<br>Valid boot device IDs can be seen by running the `bootseq` command with no options.<br>This command can only be run by users who have one or more of the following command authorities:<br>- Supervisor<br>- Blade configuration<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |

**Example:** To display the boot sequence for the compute node in node bay 2, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
bootseq -T blade[2]
```

To display information for boot device 9 for the compute node in node bay 2, while the Lenovo Flex System chassis is set as the persistent command environment, at the system> prompt, type

```
bootseq -T blade[2] -id 9
```

To set a boot sequence of PXE network (ID 6), hard disk 0 (ID 8), then floppy disk (ID 0) for the compute node in node bay 2, while the Lenovo Flex System chassis is set as the persistent command environment, at the system> prompt, type

```
bootseq -T blade[2] -seq 6|8|0
```

To set IP address information for hard disk 1 (ID 9) for the compute node in node bay 2, while the Lenovo Flex System chassis is set as the persistent command environment, at the system> prompt, type

```
bootseq -T blade[2] -id 9 -i 9.72.216.111 -g 9.72.216.1 -s 255.255.255.0
```

The following example shows the information that is returned from these commands:

```
system> bootseq -T blade[2]

Boot Order List
---------------

0 (Floppy Disk)
8 (Hard Disk 0)
6 (PXE Network)

Note:
  The max of 5 devices can be selected for boot sequence.

Available Boot Device List
--------------------------

Floppy Disk
   Presence: not installed but still selectable
   Status: active
   -id 0
   -i
   -g
   -s

Embedded Hypervisor
   Presence: not installed but still selectable
   Status: active
   -id 1
   -i
   -g
   -s

CD/DVD Rom
   Presence: not installed but still selectable
   Status: active
   -id 12
   -i
   -g
   -s

SAS
   Presence: not installed but still selectable
   Status: active
   -id 26
   -i
   -g
   -s

SAS
   Presence: not installed but still selectable
   Status: active
   -id 27
   -i
   -g
   -s

PXE Network
   Presence: not installed but still selectable
   Status: active
   -id 6
   -i
   -g
   -s

Hard Disk 0
   Presence: not installed but still selectable
   Status: active
   -id 8
   -i
   -g
   -s

Hard Disk 1
   Presence: not installed but still selectable
   Status: active
   -id 9
   -i
   -g
   -s

system> bootseq -T blade[2] -id 9

Hard Disk 1
   Presence: not installed but still selectable
   Status: active
   -id 9
   -i
   -g
   -s

system> bootseq -T blade[2] -seq 6|8|0
OK
system> bootseq -T blade[2] -id 9 -i 9.72.216.111 -g 9.72.216.1 -s 255.255.255.0
OK
system>
```

## chconfig command

This command configures the Lenovo Flex System chassis Service Advisor feature.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See “Common errors” on page 407 for a list of error messages that apply to all commands or “chconfig command errors” on page 416 for a list of error messages that are specific to the chconfig command.

*Table 17. chconfig command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display Service Advisor configuration** | Displays the contact information for the Service Advisor feature. Service Advisor resides on your CMM and monitors your Lenovo Flex System chassis for hardware events. Upon detecting a hardware event, Service Advisor captures the event, error logs, and service data, and can automatically report the event to Lenovo support. To send call home event to Lenovo support, you must enable and configure Service Advisor. For each call home event Lenovo receives, a service ticket will opened, and a follow-up call will be made. This feature will generate a message to Lenovo when events occur in the Lenovo Flex System chassis or one of its components that usually can be resolved without additional problem determination.<br>**Note:** The system will wait five days before sending duplicate events if they are left unacknowledged in the activity log. | `chconfig` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Display / accept Service Advisor terms and conditions** | Displays or accepts the terms of the Service Advisor terms and conditions. | `chconfig -li` *license*<br>where *license* is<br>• `view` to view the Service Advisor terms and conditions.<br>• `accept` to accept the Service Advisor terms and conditions.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 17. chconfig command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Enable / disable Service Advisor terms and conditions** | Enables or disables the call-home terms and conditions.<br>**Notes:**<br>• All contact information fields are required before the Service Advisor can be enabled.<br>• Call Home will connect to Lenovo service through HTTPS and HTTP. HTTP Proxy fields must be set to permit for outbound traffic.<br>• Service Advisor also needs to set up DNS server address on the CMM.<br>• Changing the Service Advisor setting from disabled to enabled will automatically trigger a test call home and the Service Advisor Activity Log will record this test call home. | `chconfig -sa` *setting* `-sc` *support_center*<br>where<br>• *setting* is<br>– `enable` to activate the Service Advisor terms and conditions.<br>– `disable` to suspend the Service Advisor terms and conditions.<br>• *support_center* is the 2character ISO 3166 country code of the Lenovo support center location. For example, the country code for the United States is US.<br><br>**Notes:**<br>• Go to http://www.iso.org/iso/country_codes/iso_3166_code_lists/ for a complete list of country codes.<br>• Valid country codes must refer to countries that have Lenovo support centers.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set contact information for Service Advisor** | Sets contact information for the Service Advisor.<br>**Note:** Each Service Advisor field can be set or updated independently, as well as specifying all fields at the same time, as shown here. | `chconfig -co "`*company*`" -cn "`*name*`"-cph "`*phone*`" -cphe "`*extension*`"-ce` *email* `-mlph "`*m_phone*`"-ca "`*address*`"-cci "`*city*`"-cs` *state*`-sc` *support_center*`-cz "`*postalcode*`"`<br>where:<br>• "*company*" is the quote-delimited contact company | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 17. chconfig command (continued)*

| **Function** | **What it does** | **Command** | **Target** *(see paths in* "Command targets" *on page 6)* |
|---|---|---|---|
| | | name, of up to 30 characters in length.<br>• "*name*" is the quote-delimited contact name, of 1 to 30 characters in length.<br>• "*phone*" is the quote-delimited contact phone number, of 5 to 30 characters in length.<br>• "*extension*" is the quote-delimited contact phone extension, of 1 to 30 characters in length.<br>• *email* is email address of the contact person in the form userid@hostname (30 characters maximum). The userid can be alphanumeric characters, ".", "-", or "_" but must begin and end with alphanumeric characters. The hostname can be alphanumeric characters, ".", "-", or "_". It must contain at least two domain items. Every domain item should begin and end with an alphanumeric character and the last domain item should be from 2 to 20 alphabetic characters.<br>• "*m_phone*" is the quote-delimited machine location phone number, of 5 to 30 characters in length.<br>*(continued on next page)* | |
| **Set contact information for Service Advisor** *(continued)* | | • "*address*" is the quote-delimited street address of the machine location, of 1 to 30 characters in length.<br>• "*city*" is the quote-delimited city of the machine location, of 1 | |

Table 17. chconfig command (continued)

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | | to 30 characters in length.<br>• *state* is the state of the machine location, of 2 to 3 characters in length.<br>• "*postalcode*" is the quote-delimited postal code of the machine location, of 1 to 9 alphanumeric characters in length.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | |
| **Set contact information for alternate Service Advisor** | Sets contact information for an alternate Service Advisor.<br>**Note:** Each alternate Service Advisor field can be set or updated independently, as well as specifying all fields at the same time, as shown here. | `chconfig -acn` "*name*" `-acph` "*phone*" `-acphe` "*extension*"`-ace` *email* `-mlph` "*m_phone*" `-ca` "*address*" `-cci` "*city*"`-cs` *state*`-sc` *support_center*`-cz` "*postalcode*"<br>where:<br>• "*name*" is the quote-delimited contact name, of 1 to 30 characters in length.<br>• "*phone*" is the quote-delimited contact phone number, of 5 to 30 characters in length.<br>• "*extension*" is the quote-delimited contact phone extension, of 1 to 30 characters in length.<br>• *email* is email address of the contact person in the form userid@hostname (30 characters maximum). The userid can be alphanumeric characters, ".", "-", or "_" but must begin and end with alphanumeric characters. The hostname can be | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 17. chconfig command (continued)*

| Function | What it does | Command | **Target** *(see paths in "*Command targets*" on page 6)* |
|---|---|---|---|
| | | alphanumeric characters, ".", "-", or "_". It must contain at least two domain items. Every domain item should begin and end with an alphanumeric character and the last domain item should be from 2 to 20 alphabetic characters.<br>• "*m_phone*" is the quote-delimited machine location phone number, of 5 to 30 characters in length.<br>• "*address*" is the quote-delimited street address of the machine location, of 1 to 30 characters in length.<br>*(continued on next page)* | |
| **Set contact information for alternate Service Advisor** *(continued)* | | • "*city*" is the quote-delimited city of the machine location, of 1 to 30 characters in length.<br>• *state* is the state of the machine location, of 2 to 3 characters in length.<br>• "*postalcode*" is the quote-delimited postal code of the machine location, of 1 to 9 alphanumeric characters in length.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | |

*Table 17. chconfig command (continued)*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set up HTTP proxy for Service Advisor** | Sets up HTTP proxy for Service Advisor. | `chconfig -ps` *setting*`-loc` *hostname*`-po` *port*`-u` *"username"*`-pw` *"password"*<br>where:<br>• *setting* is `enabled` or `disabled`<br>• *hostname* is the fully qualified host name or IP address of the HTTP proxy, of 1 to 63 characters in length.<br>• *port* is the port of the HTTP proxy, a number from 1 to 65535, inclusive.<br>• *"username"* is the quote-delimited user name, of 1 to 30 characters in length.<br>• *"password"* is the quote-delimited password of the HTTP proxy, of up to 15 characters in length<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

**Example:**

To accept the Service Advisor terms and conditions, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
chconfig -li accept -T mm[p]
```

To display the current configuration of the Service Advisor, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
chconfig -T mm[p]
```

The following example shows the information that is returned from these two commands:

```
system> chconfig -li accept -T mm[p]
OK
system> chconfig -T mm[p]
```

```
-sa enabled
-sc  US
-ca  No 399, Keyuan Rd,
-cci  Dallas
-ce  bob@lenovo.com
-cn  bob
-co  Lenovo
-cph  800-555-1111
-cs  TX
-cz  75210
-cphe  5678
-acn  mary
-acph  800-555-1113
-acphe  1234
-ace  mary@lenovo.com
-mlph  800-555-1112
-loc  google.cn
-po  8080
-ps disabled
-u  User-001
system>
```

## chlog command

This command is used to display up to five call-home activity log entries and to mark a call-home event entry as acknowledged or unacknowledged.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See “Common errors” on page 407 for a list of error messages that apply to all commands or “chlog command errors” on page 418 for a list of error messages that are specific to the chlog command.

Table 18. *chlog (display call-home activity log) command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display call-home activity log entries** | Displays the last fifty entries from the call-home activity log.<br>**Notes:**<br>• The entries are displayed in reverse chronological order (most recent call-home entry first).<br>• The system will wait 5 days before sending duplicate events if they are not acknowledged as corrected in the activity log.<br>• Call-home events are usually those that can be resolved without additional problem determination. | `chlog` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Display FTP/TFTP server call-home activity log entries** | Displays the last fifty FTP/TFTP server entries from the call-home activity log.<br>**Notes:**<br>• The entries are displayed in reverse chronological order (most recent call-home entry first).<br>• The system will wait 5 days before sending duplicate events if they are not acknowledged as corrected in the activity log. | `chlog -f` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 18. chlog (display call-home activity log) command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display Lenovo Support call-home activity log entries** | Displays the last five Lenovo Support entries from the call-home activity log.<br>**Notes:**<br>• The entries are displayed in reverse chronological order (most recent call-home entry first).<br>• The system will wait 5 days before sending duplicate events if they are not acknowledged as corrected in the activity log.<br>• Call-home events are usually those that can be resolved without additional problem determination. | `chlog -s` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Acknowledge / unacknowledge call-home activity log entries** | Marks the selected call-home event as acknowledged (yes) or unacknowledged (no) when the call-home event has been corrected.<br>**Note:** The system will wait five days before sending duplicate events if they are left unacknowledged in the activity log. | `chlog` -*index*`-ack` *option*<br>where:<br>• *index* is the index of the call-home event entry<br>• *option* is `yes` or `no`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

**Example:**To display the last five call-home activity log entries, while the primary CMM in bay 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
chlog
```

To mark the call-home event with index number 14 as acknowledged, type

```
chlog -14 -ack yes
```

The following example shows the information that is returned from these two commands:

```
system:mm[1]> chlog
Index  Ack  Send Result   Assigned Num  Event ID    Sev  Source
            Time                  Message
14     No   Success        NULL         0x00016802  I    CHASSIS
06/04/11  09:11:11   Test Call Home generated  by USERID.
15     No   Pending       NULL         0x00016802  I    CHASSIS
06/04/11  09:11:12   Test Call Home generated  by USERID.

system:mm[1]>chlog -14 -ack yes
OK
system:mm[1]>
```

## chmanual command

This command tests the Lenovo Flex System chassis call-home feature setup.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "chmanual command errors" on page 418 for a list of error messages that are specific to the chmanual command.

*Table 19. chmanual command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Create call-home problem message** | Create a call-home problem message for a CMM or compute node. | `chmanual -desc "`*description*`"`<br>where "*description*" is a quote-delimited problem description of 1 to 100 characters in length.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>• Chassis log management<br>• Chassis administration<br>• Chassis configuration<br>• Blade administration<br>• Blade configuration<br>• Blade remote presence<br>• I/O module administration<br>• I/O module configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system`<br>Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |
| **Generate call-home test call home** | Manually generate a test call-home event that transmits the sample call-home problem message. | `chmanual -test`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>• Chassis log management<br>• Chassis administration<br>• Chassis configuration<br>• Blade administration<br>• Blade configuration<br>• Blade remote presence<br>• I/O module administration<br>• I/O module configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system` |

**Example:**

To create a call-home test message, at the system:> prompt, type

```
chmanual -desc "This is a test."
```

To manually send a test message, while the system is set as the persistent command environment, at the system> prompt, type

```
chmanual -test
```

The following example shows the information that is returned from these two commands:

```
system> chmanual -desc "This is a test."
OK
system> chmanual -test
OK
system>
```

## cimsub command

This command displays and clears subscriptions for the common information model (CIM) used by the optional Lenovo XClarity Administrator or Flex System Manager software.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "cimsub command errors " on page 419 for a list of error messages that are specific to the cimsub command.

*Table 20. cimsub command*

| Function | What it does | Command | **Target** *(see paths in* "Command targets" *on page 6)* |
|---|---|---|---|
| **Display CIM subscription destination** | Displays destinations for the CIM subscriptions used by the Lenovo XClarity Administrator or Flex System Manager software. | `cimsub` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Display CIM subscription status** | Displays detailed information about all CIM subscriptions used by the Lenovo XClarity Administrator or Flex System Manager software. | `cimsub -v` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Clear CIM subscription** | Clears one or all of the CIM subscriptions used by the Lenovo XClarity Administrator or Flex System Manager software. | `cimsub -clear` *identifier*<br>where *identifier* is:<br>• `all` to delete all subscriptions.<br>• a single destination URL identifer contained within double-quotes. Valid subscription identifiers can be seen by running the `cimsub` command with no arguments or the `cimsub -v` command.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

**Example:**

To display CIM destinations for the primary CMM, while the Lenovo Flex System chassis is set as the persistent environment, at the `system>` prompt, type

```
cimsub -T mm[p]
```

To display CIM status for the primary CMM, while the Lenovo Flex System chassis is set as the persistent environment, at the `system>` prompt, type

```
cimsub -v -T mm[p]
```

To clear the CIM subscription with an identifier of http://9.37.64.50:8080 for the primary CMM, while the Lenovo Flex System chassis is set as the persistent environment, at the `system>` prompt, type

```
cimsub -clear "http://9.37.64.50:8080" -T mm[p]
```

To clear all CIM subscriptions for the primary CMM, while the Lenovo Flex System chassis is set as the persistent environment, at the `system>` prompt, type

```
cimsub -clear all -T mm[p]
```

The following example shows the information that is returned from these commands:

```
system> cimsub -T mm[p]
Destination = "http://9.37.64.50:8080"

Destination = "http://9.37.64.50:8080"

system> cimsub -v -T mm[p]
Caption = NULL
CreationClassName = "CIM_ListenerDestinationCIMXML"
Description = NULL
Destination = "http://9.37.64.50:8080"
ElementName = "Listener"
InstanceID = NULL
Name = "TEST:Indications:AllEvents"
OtherPersistenceType = NULL
OtherProtocol = NULL
PersistenceType = 2
Protocol = 2
SystemCreationClassName = "CIM_ComputerSystem"
Filter = "root/interop:CIM_IndicationFilter.CreationClassName=\"CIM_IndicationFil
ter\",Name=\"TEST:Indications:AllEvents\",SystemCreationClassName=\"CIM_ComputerS
ystem\",SystemName=\"\""
FailureTriggerTimeInterval = 3600
OnFatalErrorPolicy = 2
OtherRepeatNotificationPolicy = NULL
OtherSubscriptionState = NULL
RepeatNotificationCount = NULL
RepeatNotificationGap = NULL
RepeatNotificationInterval = NULL
RepeatNotificationPolicy = 2
SubscriptionDuration = NULL
SubscriptionState = 2
SubscriptionTimeRemaining = NULL
TimeOfLastStateChange = "20150212160444.680645-300"
Caption = NULL
CreationClassName = "CIM_IndicationFilter"
Description = NULL
ElementName = "Filter"
IndividualSubscriptionSupported = TRUE
InstanceID = NULL
Name = "TEST:Indications:AllEvents"
Query = "SELECT*FROMCIM_AlertIndication"
QueryLanguage = "WQL"
SourceNameSpaces = {"root/cimv2"}
SourceNameSpace =
SystemCreationClassName = "CIM_ComputerSystem"
SystemName = "localhost"

Caption = NULL
```

```
CreationClassName = "CIM_ListenerDestinationCIMXML"
Description = NULL
Destination = "http://9.37.64.50:8080"
ElementName = "Listener"
InstanceID = NULL
Name = "TEST2:Indications:AllEvents"
OtherPersistenceType = NULL
OtherProtocol = NULL
PersistenceType = 2
Protocol = 2
SystemCreationClassName = "CIM_ComputerSystem"
Filter = "root/interop:CIM_IndicationFilter.CreationClassName=\"CIM_IndicationFil
ter\",Name=\"TEST2:Indications:AllEvents\",SystemCreationClassName=\"CIM_Computer
System\",SystemName=\"\""
FailureTriggerTimeInterval = 3600
OnFatalErrorPolicy = 2
OtherRepeatNotificationPolicy = NULL
OtherSubscriptionState = NULL
RepeatNotificationCount = NULL
RepeatNotificationGap = NULL
RepeatNotificationInterval = NULL
RepeatNotificationPolicy = 2
SubscriptionDuration = NULL
SubscriptionState = 2
SubscriptionTimeRemaining = NULL
TimeOfLastStateChange = "20150212160559.819293-300"
Caption = NULL
CreationClassName = "CIM_IndicationFilter"
Description = NULL
ElementName = "Filter"
IndividualSubscriptionSupported = TRUE
InstanceID = NULL
Name = "TEST2:Indications:AllEvents"
Query = "SELECT*FROMCIM_AlertIndication"
QueryLanguage = "WQL"
SourceNameSpaces = {"root/cimv2"}
SourceNameSpace =
SystemCreationClassName = "CIM_ComputerSystem"
SystemName = "localhost"

system> cimsub -clear "http://9.37.64.50:8080" -T mm[p]
OK
system> cimsub -clear all -T mm[p]
OK
system>
system> cimsub -T mm[p]
No CIM subscription info available
system>
```

## cin command

This command can be used to view and configure the chassis internal network for up to 14 supported chassis internal network (CIN) configurations, globally, or for specified entries. You can define a CIN by creating a pool of VLAN (virtual local area network) ID/IP address pairs, each of which is a CIN entry.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See “Common errors” on page 407 for a list of error messages that apply to all commands or “cin command errors ” on page 419 for a list of error messages that are specific to the cin command.

*Table 21. cin command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display CIN configuration table** | Displays the configuration table for the chassis internal network. Possible return values are:<br>• Global CIN enabled or disabled status<br>• CIN index<br>– VLAN ID<br>– IP address<br>– index entry enabled or disabled status | `cin` | Lenovo Flex System chassis:<br>`system` |
| **Set global CIN state** | Sets the global state of CIN to enabled or disabled. | `cin -global -en` *state*<br>where *state* is<br>• `on`<br>• `off`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management and chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system` |
| **Clear all CIN configuration entries** | Deletes all CIN configuration entries. | `cin all -clear`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management and chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system` |

*Table 21. cin command (continued)*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Turn all index entries on or off** | Turns all CIN index entries on or off. | `cin all -en` *state*<br>where *state* is<br>- `on`<br>- `off`<br>This command can only be run by users who have one or more of the following command authorities:<br>- Supervisor<br>- Chassis account management and chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system` |
| **Delete CIN configuration entry** | Deletes the specified CIN configuration entry. | `cin` -*entry_index*`-clear`<br>where *entry_index* is a number between 1 and 14 (inclusive).<br>This command can only be run by users who have one or more of the following command authorities:<br>- Supervisor<br>- Chassis account management and chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system` |

*Table 21. cin command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set CIN configuration entry to enable or disable** | Enables or disables a CIN configuration entry.<br>If you attempt to enable or disable a non-existent entry, the action is ignored and no error message is returned. | `cin` -*entry_index*`-en` *state*<br>where:<br>• *entry_index* is a number between 1 and 14, and<br>• *state* is<br>– `on`<br>– `off`<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management and chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system` |
| **Create a CIN configuration entry** | Creates a CIN index entry.<br>If the CIN index is currently empty, both -id and -ip must be specified.<br><br>**Note:** The VLAN ID must be different from that of the compute nodeCMM. | `cin` -*entry_index* -id *vlan_id*`-ip` *ip_address*<br>where:<br>• *entry_index* is a number between 1 and 14,<br>• *vlan_id* is a VLAN ID number between 3 and 4094 (inclusive),<br>• *ip_address* is a valid IP address.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management and chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system` |

Table 21. cin command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Specify valid IP address for CIN index entry** | Specifies the IP address of the CIN index entry. The CIN IP address must be a valid IP address. An error is displayed if the IP address is invalid.<br>**Notes:**<br>• If the index is not empty, the IP address can be specified separately.<br>• CIN entries cannot have matching IP addresses unless they are 0.0.0.0. and have different VLAN IDs.<br>• If the CIN IP address is 0.0.0.0, the compute node IP address for CIN which is configured in the compute node operating system cannot be in the same subnet as that of the CMM.<br>• The IP address cannot be multi-cast and cannot match the IP address of the CMM. | `cin` -*entry_index*`-ip` *ip_address*<br>where:<br>• *entry_index* is a number between 1 and 14<br>• *ip_address* is a valid IP address.<br>You can overwrite parameters of an existing definition; for example, cin -1 -ip 0.0.0.0 overwrites the current CIN IP address of the first cin entry. If the entry does not exist, an error is returned.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management and chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system` |
| **Specify VLAN ID for CIN entry** | Set the VLAN ID for the specified CIN entry.<br>**Notes:**<br>• If the index is not empty, the ID can be specified separately.<br>• The VLAN ID must be different from that of the CMM. | `cin` -*entry_index*`-id` *vlan_id*<br>where:<br>• *entry_index* is a number between 1 and 14<br>• *vlan_id* is a number between 3 and 4094 (inclusive).<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management and chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system` |

**Example:**

To view chassis internal network information for the CMM, while this CMM is set at the persistent command environment, at the `system>` prompt, type
`cin`

The following example shows the information that is returned from this command:

```
system> cin
 -global -en off

Index 1
 -id 11
 -ip 11.1.1.1
 -en on

Index 2
 -id 12
 -ip 22.1.1.1
 -en on

Index 3
 not used

Index 4
 not used

Index 5
 not used

Index 6
 not used

Index 7
 not used

Index 8
 not used

Index 9
 not used

Index 10
 not used

Index 11
 not used

Index 12
 -id 123
 -ip 23.1.1.1
 -en on

Index 13
 not used

Index 14
 not used
system>
```

## cinstatus command

This command displays a table listing the VLAN ID, the IP address, the MAC address, and the status of each chassis internal network (CIN) connection.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "cinstatus command errors " on page 420 for a list of error messages that are specific to the cinstatus command.

*Table 22. cinstatus command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display entries of the CIN status table** | Reads entries of the CIN status table, five at a time. Each entry of the table returns:<br>• CIN VLAN ID<br>• CIN IP address<br>• CIN MAC address<br>• CIN status text<br>**Note:** An asterisk ( * ) shown next to an IP address indicates that it is a learned value. | `cinstatus` | Lenovo Flex System chassis:<br>`system` |
| **Display status of first five CIN entries** | Displays the first five entries of the CIN status table. | `cinstatus -f` | Lenovo Flex System chassis:<br>`system` |
| **Display entire CIN status table** | Displays all the entries in the CIN status table. | `cinstatus -a` | Lenovo Flex System chassis:<br>`system` |

**Example:**

To display five entries of the CIN status table, while the Lenovo Flex System chassis is set as the persistent environment, at the `system>` prompt, type
`cinstatus`

The following example shows the information that is returned from this command

```
system> cinstatus
    Note: * next to IP address indicates a learned entry

    VLAN IP Address        MAC Address        Status
    ---- ---------------  ----------------- -------------------
 1. 4094 0.0.0.1                            Not Operational
 2. 4094 0.0.0.2                            Not Operational
 3. 4    0.0.0.0                            Operational
 4. 4093 0.0.0.1                            Not Operational
 5. 4094 0.0.0.0                            Operational

 Last entry reached
system>
```

## clear command

This command restores the primary CMM configuration or an I/O (switch) module configuration to the manufacturing default settings.

**Notes:**

- The command must always include the `-cnfg` option.
- To restore a saved CMM configuration after restoring the manufacturing default settings, use the **read** command (see "read command" on page 280 for information about command use).

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "clear command errors" on page 421 for a list of error messages that are specific to the clear command.

*Table 23. clear command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Restore default configuration of primary CMM and keep logs** | Restores the default configuration of the primary CMM, retaining log information; then, resets the CMM. If the current operating state of the Lenovo Flex System chassis indicates potential problems with restoring the default configuration, an error message is returned and the restore is cancelled.<br>No results are returned from this command because it resets the CMM.<br>When you restore the CMM configuration, the Ethernet configuration method is set to a value of dthens. After the CMM resets, this causes the CMM to try dhcp configuration and then default to the static IP configuration, which might cause the CMM to remain offline for longer than normal. See the "ifconfig command" on page 174 for information. | `clear -cnfg`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis administration and chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Restore default configuration of primary CMM and keep logs (with override)** | Restores the default configuration of the primary CMM, retaining log information; then, resets the CMM, overriding error messages and restoration cancellation due to the current Lenovo Flex System chassis operating state.<br>No results are returned from this command because it resets the CMM.<br>When you restore the CMM configuration, the Ethernet configuration method is set to a value of dthens. After the CMM resets, this causes the CMM to try dhcp configuration and then default to the static IP configuration, which might cause the CMM to remain offline for longer than normal. See the "ifconfig command" on page 174 for information. | `clear -cnfg -o`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis administration and chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Restore default configuration of I/O module** | Restores the configuration of the specified I/O module to the default settings. | `clear -cnfg`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor | I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |

*Table 23. clear command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | | • I/O module administration and I/O module configuration<br>See "Commands and user authority" on page 10 for additional information. | |

**Example:** To restore the primary CMM configuration to default settings and retain log information, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
clear -cnfg -T mm[p]
```

No results are returned from this command. After the primary CMM resets, you will need to start a new command-line session.

## clearlog command

This command clears the CMM audit event log, the system event log, or both.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "clearlog command errors" on page 422 for a list of error messages that are specific to the clearlog command.

Table 24. clearlog (clear CMM event log) command

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Clear CMM event log** | Clears the both the CMM audit event log and the CMM system event log, displaying a message confirming that both event logs were cleared.<br>**Notes:**<br>• Audit log events are created by the actions of users.<br>• Although system events and audit events are stored internally in separate log files, they are presented to the user as a single log that can be filtered.<br>• If you clear both logs, an entry indicating you cleared the audit log is shown in the audit log and an entry indicating you cleared the system log is shown in the system log. | `clearlog`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis log management<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Clear CMM audit or system event log** | Clears the CMM audit event log, the system event log, or both, and displays a message confirming that the specified event log was cleared.<br>**Notes:**<br>• Audit log events are created by the actions of users.<br>• If the *log_type* is not specified, this command will clear both logs.<br>• Although system events and audit events are stored internally in separate log files, they are presented to the user as a single log that can be filtered.<br>• If you clear the audit log, an entry indicating you cleared the audit log is shown in the audit log. If you clear the system log, an entry indicating you cleared the system log is shown in the system log. If you clear both logs, an entry indicating you cleared the audit log is shown in the audit log and an entry indicating you cleared the system log is shown in the system log. | `clearlog -l` *log_type*<br>where *log_type* is `audit` or `system`.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis log management<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

**Example:** To clear both the CMM audit log and the CMM system event log, while the primary CMM in bay 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
clearlog
```

To clear the CMM audit log, while the primary CMM in bay 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
clearlog -1 audit
```

To clear the CMM system event log, while the primary CMM in bay 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
clearlog -1 system
```

The following examples shows the information that is returned from these commands:

```
system:mm[1]> clearlog -1 audit
OK
I  Audit     (CMM 02) The Audit log has been cleared by user ID USERID from SSH at address 9.42.104.88.
I  SERVPROC  (CMM 02) The Event log has been cleared by user ID USERID from SSH at address 9.42.104.88.
system:mm[1]>clearlog -1 audit
OK
I  Audit     (CMM 02) The Audit log has been cleared by user ID USERID from SSH at address 9.42.104.88.
clearlog -1 system
OK
I  SERVPROC  (CMM 02) The Event log has been cleared by user ID USERID from SSH at address 9.42.104.88.
```

## config command

This command sets and displays the name of the CMM or compute node and the location and contact name for the CMM.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "config command errors" on page 422 for a list of error messages that are specific to the config command.

*Table 25. config command*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display identifying information for Lenovo Flex System chassis** | Displays the following information for the command target:<br>• Name<br>• Room<br>• Rack<br>• Rack unit | `config` | Lenovo Flex System chassis:<br>`system` |
| **Display name of compute node** | Displays the name of the specified compute node. | `config` | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |
| **Display name of CMM** | Displays the following information for the command target:<br>• Name<br>• Location<br>• Contact name | `config` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 25. config command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set name of chassis** | Sets the name of the chassis. | `config -name` "*name*"<br>where "*name*" is up to 15 characters in length and contained within double-quotes. Any printable character can be used in the chassis name.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system` |
| **Set name of CMM** | Sets the name of the primary CMM. | `config -name` *name*<br>where *name* is up to 15 characters in length.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration (for CMM)<br>• Blade configuration (for compute node)<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 25. config command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set name of compute node** | Sets the name of the specified compute node. | `config -name "`*name*`"`<br>where "*name*" is up to 15 characters in length and contained within double-quotes.<br>Names can contain any character other than "<" and ">".<br>Names can contain spaces.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade configuration<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |
| **Set rack location of chassis** | Sets the rack where the chassis is located. | `config -rack "`*rack*`"`<br>where "*rack*" is up to 23 characters in length and contained within double-quotes.<br>Rack locations can contain any character other than "<" and ">".<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system` |

*Table 25. config command (continued)*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set rack unit location of chassis** | Sets the lowest rack unit that the chassis occupies in a rack. | `config -rackunit` "*unit*" where "*unit*" is an integer between 0 and 99, inclusive, that identifies the lowest unit of a rack that the chassis occupies.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system` |
| **Set room location of chassis** | Sets the room where the chassis is located. | `config -room` "*room*" where "*room*" is up to 23 characters in length and contained within double-quotes.<br>Room locations can contain any character other than "<" and ">".<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system` |

Table 25. config command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set location of CMM** | Sets the location of the primary CMM. | `config -loc` "*location*"<br>where "*location*" is up to 47 characters in length and contained within double-quotes.<br>CMM locations can contain any character other than "<" and ">".<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set contact name for CMM** | Sets the contact name for the primary CMM. | `config -contact` "*contact_name*"<br>where "*contact_name*" is up to 47 characters in length and contained within double-quotes.<br>CMM contact names can contain any character other than "<" and ">".<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

**Example:**

To set the primary CMM name to Lenovo_lab, while the Lenovo Flex System chassis is set as the persistent command environment, at the system> prompt, type

```
config -name Lenovo_lab -T mm[p]
```

To display the primary CMM name, location, and contact name, while the Lenovo Flex System chassis is set as the persistent command environment, at the system> prompt, type

```
config -T mm[p]
```

The following example shows the information that is returned from these two commands:

```
system> config -name Lenovo_lab -T mm[p]
OK
system> config -T mm[p]
-name Lenovo_lab
-contact John_Doe
-loc Main_Lab
system>
```

## console command

This command sets up a serial over LAN connection to the command console of a compute node.

To end an SOL session, press Esc followed by an open parenthesis:

Esc (

**Note:** See your operating-system documentation for information about SOL commands that you can enter by using the CMM command-line interface.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "console command errors" on page 423 for a list of error messages that are specific to the console command.

*Table 26. console command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Create SOL session with compute node** | Creates an SOL connection to the specified compute node.<br>**Note:** The CMM supports a persistent SOL connection that remains intact until you escape from the SOL console, or another user uses the override option to take over your SOL console. A persistent command, if dropped, automatically attempts to reconnect. | `console`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade remote presence<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |
| **Create override SOL session with compute node** | Creates an SOL connection to the specified compute node, with the override option enabled. This enables you to end an existing SOL session to that compute node and start a new one.<br>**Note:** The CMM supports combining this option with the -l option to override an existing session, and not reconnect if the connection drops. | `console -o`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade remote presence<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |
| **Create non-persistent SOL session with compute node** | Creates an SOL connection to the specified compute node for users who do not want to use a persistent session.<br>**Note:** This option can be combined with the -o option to override an existing session, and not reconnect if the connection drops. | `console -l`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade remote presence<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |

**Example:** To start an SOL connection to the compute node in node bay 14, while this compute node is set as the persistent command environment, at the `system:mm[x]>` prompt, type

```
console -T system:blade[14]
```

## coolingzones command

This command displays Lenovo Flex System chassis cooling zone and fan module health information.

**Note:** If one or more fan modules in a cooling zone are missing, the components installed in that cooling zone might not cool sufficiently. Check the CMM event log for temperature event messages using the "displaylog command" on page 119.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "coolingzones command errors " on page 423 for a list of error messages that are specific to the coolingzones command.

*Table 27. coolingzones command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display cooling zone information** | Display information for all cooling zones in the Lenovo Flex System chassis. | `coolingzones` | Lenovo Flex System chassis:<br>`system` |
| **Display specific cooling zone information** | Displays detailed information for the specified cooling zone. | `coolingzones z` *zone* where *zone* is the cooling zone index number to display.<br>Valid cooling zone index numbers can be seen by running the `coolingzones` command with no argument. | Lenovo Flex System chassis:<br>`system` |

**Example:** To display cooling zone information for all cooling zones, while the chassis is set as the persistent command environment, at the `system>` prompt, type
`coolingzones`

To display cooling zone information for cooling zone 2, while the chassis is set as the persistent command environment, at the `system>` prompt, type
`coolingzones z2`

The following example shows the information that is returned from these commands:

```
system> coolingzones

Zone 1:
-------
Status: ok
Provider(s):
      blower[1]
      blower[2]
      blower[3]
      blower[4]
Receiver(s):
      blade[5],blade[11]

Zone 2:
-------
Status: warning
Provider(s):
      blower[6] not present
      blower[7]
      blower[8]
      blower[9]
Receiver(s):
      blade[4]

Zone 3:
-------
Status: warning
Provider(s):
      blower[5] not present
```

```
Receiver(s):
      mm[1]
      switch[2]

Zone 4:
-------
Status: ok
Provider(s):
      blower[10]
Receiver(s):
      switch[1],switch[3]

system> coolingzones z2

Status: warning

Cooling Provider(s):
--------------------

blower[6]: not present
blower[7]:
      Status: ok
      Count: 1
      Speed: 38%
      Avg RPM: 4352
      Controller State: Operational
blower[8]:
      Status: ok
      Count: 1
      Speed: 38%
      Avg RPM: 4352
      Controller State: Operational
blower[9]:
      Status: ok
      Count: 1
      Speed: 38%
      Avg RPM: 4416
      Controller State: Operational

Cooling Receiver(s):
--------------------

  blade[4]

system>
```

## crypto command

This command displays and configures the cryptographic settings for the CMM. These settings are required to achieve National Institute of Standards and Technology (NIST) compatibility.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See “Common errors” on page 407 for a list of error messages that apply to all commands or “crypto command errors” on page 424 for a list of error messages that are specific to the crypto command.

For more information about NIST, see "Configuring NIST 800-131A compliance" in the *Lenovo Chassis Management Module 2 User's Guide*.

*Table 28. crypto command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display CMM cryptographic settings** | Displays the cryptographic settings for the CMM. Return values include the currently selected CMM cipher suite, cryptographic mode, and the cryptographic mode specification version. | `crypto` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set CMM cipher suites** | Sets the allowed cipher suites for the primary CMM either to those defined by the TLS 1.2 specification (effectively limiting communication to TLS 1.2 only) or to a broader set of cipher suites that can be used with SSL 3.0, TLS 1.0, TLS 1.1, or TLS 1.2.<br>**Important:**<br>• If the `-cs` command option is run by itself, all secure connections are closed and will need to be reestablished after a successful cipher suite change.<br>• If the `-cs` and `-m` command options are run together, the CMM automatically restarts after a successful cipher suite and cryptographic mode change.<br>**Notes:**<br>• To set the cipher suite setting to `legacy`, the cryptographic mode must be set to `comp` (compatibility with all NIST cipher suites).<br>• The cipher suite cannot be changed from `tls1.2` to `tls1.2srv` when the cryptographic mode is set to `nist800-131a`.<br>• The cipher suite setting (`-cs`) is referred to as the TLS/SSL setting in the CMM Web interface (**Mgt Module Management > Security > Cryptography**). | `crypto -cs` *cipher*<br>where *cipher* is:<br>• `legacy` for legacy cryptographic settings (such as SSL)<br>• `tls1.2` for NIST Transport Layer Security (TLS) 1.2 cryptography on both the client and server<br>• `tls1.2svr` for NIST Transport Layer Security (TLS) 1.2 cryptography on only the server<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set CMM cryptographic mode** | Sets the cryptographic mode for the primary CMM.<br>**Notes:**<br>• To set the cryptographic mode to `nist800-131a`, the cipher suite setting must be set to `tls1.2` or `tls1.2svr`.<br>• If the `crypto -m` option is set to `comp` (compatibility with all NIST cipher suites), the `sslcfg -ca` | `crypto -m` *mode*<br>where *mode* is:<br>• `comp` for compatibility with all NIST cipher suites set by the `cipher -cs` command option.<br>• `nist800-131a` for compatibility with only the NIST Transport Layer Security (TLS) | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 28. crypto command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
|  | `-csa` option must be specified when generating a CA certificate (see the "sslcfg command" on page 328 for more information).<br>• The CMM automatically restarts after a successful cryptographic mode change. | 1.2 cipher suites set by the `cipher -cs` command option.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. |  |

**Example:**

To display the cryptographic settings for the primary CMM, while the primary CMM in bay 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type
`crypto`

To set the cryptographic setting for the primary CMM to Transport Layer Security (TLS) 1.2, while the primary CMM in bay 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type
`crypto -cs tls1.2`

To set the cryptographic setting for the primary CMM to use the legacy settings, while the primary CMM in bay 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type
`crypto -cs legacy`

The following example shows the information that is returned from these commands, when they are run using a Telnet connection:

```
system:mm[1]> crypto
-cs legacy
-m comp
Version: 01.00
system:mm[1]> crypto -cs tls1.2
Affected services will now be restarted. All secure sessions will be
closed, and need to be reestablished.
OK
system:mm[1]> crypto
-cs tls1.2
-m comp
Version: 01.00
system:mm[1]> crypto -cs legacy
Affected services will now be restarted. All secure sessions will be
closed, and need to be reestablished.
OK
system:mm[1]> crypto
-cs legacy
-m comp
Version: 01.00
system:mm[1]>
```

## date command

This command configures and displays the CMM date settings.

**Note:** The `date` command replaces the `clock` command that was used in previous CMM firmware versions.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "date command errors" on page 425 for a list of error messages that are specific to the date command.

*Table 29. date command*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "*Command targets*" on page 6)* |
|---|---|---|---|
| **Display CMM clock information** | Displays the following information for the CMM clock:<br>• current date and time<br>• GMT (Greenwich-Mean Time) offset<br>• daylight-savings time setting | `date` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Display valid timezone settings** | Displays list of available timezone settings for the CMM clock, with limited information about each time zone. The CMM supports more than 400 geography-based timezone settings. | `date -tz all` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Display valid timezone settings (verbose)** | Displays list of available timezone settings for the CMM clock, with detailed information about each time zone. The CMM supports more than 400 geography-based timezone settings.<br>**Note:** The `-v` command option must be used with the `date -tz all` command option. | `date -tz all -v` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 29. date command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set CMM date** | Sets the date for the CMM clock. | `date -d` *date*<br>where *date* is the current calendar date in mm/dd/yyyy format.<br>The month and day can be input as single digits. The year must be a four-digit number between 1970 and 2037 inclusive.<br>This command can only be run by users who have the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set CMM time** | Sets the time for the CMM clock. | `date -t` *time*<br>where *time* is the current time in 24-hour hh:mm:ss format.<br>The hours, minutes, and seconds can all be input as single digits.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set CMM clock time zone** | Sets the time zone for the CMM clock.<br>**Note:** The daylight-savings time setting for your time zone is set automatically. | `date -tz` *timezone*<br>where *timezone* is one of the valid time zone values listed by the `date -tz all` command.<br>This command can only be run by users who have the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

**Example:** To set the primary CMM for operation in the US Eastern time zone, with a current date of 08/15/2015 and time of 10:38:00, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
date -T mm[p] -tz America/New_York -t 10:38:00 -d 08/15/2015
```

To display the clock information for the primary CMM, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
date -T mm[p]
```

To display detailed time zone information for the Abidjan time zone in Africa, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
date -T mm[p] -tz Africa/Abidjan -v
```

The following example shows the information that is returned from these commands:

```
system> date -T mm[p] -tz America/New_York -t 10:38:00 -d 08/15/2015
OK
system> date -T mm[p]
08/15/2015 10:38:03 America/New_York (Eastern Time) DST is currently being observed
system> date -T mm[p] -tz Africa/Abidjan -v

Timezone name: Africa/Abidjan
Timezone Standard name: Africa/Abidjan Time
Timezone standard caption: GMT
Timezone CMM offset: UTC
No daylight saving time in 2015
system>
```

## dhcpinfo command

This command displays the IP configuration that is assigned by a DHCP server to the primary CMM external network interface, compute node management network interfaces, and I/O module DHCPv6 server.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "dhcpinfo command errors" on page 426 for a list of error messages that are specific to the dhcpinfo command.

*Table 30. dhcpinfo command*

| Function | What it does | Command | **Target** *(see paths in "*Command targets*" on page 6)* |
|---|---|---|---|
| **Display Ethernet channel 0 DHCP configuration for primary CMM** | If the IP configuration for the primary CMM eth0 is assigned by a DHCP server, the configuration that is assigned by the DHCP server and DHCP server information is displayed. If the IP configuration for eth0 is *not* assigned by a DHCP server, an error message is displayed. Possible configuration values returned are:<br>• -server *dhcp_ip_address*<br>• -n *hostname*<br>• -i *ip_address*<br>• -g *gateway_address*<br>• -s *subnet_mask*<br>• -d *domainname*<br>• -dns1 *primary_dns_ip_address*<br>• -dns2 *secondary_dns_ip_address*<br>• -dns3 *tertiary_dns_ip_1address*<br>• -server6 *IPv6_dhcp_ip_address*<br>• -i6 *IPv6_address*<br>• -d6 *IPv6_domainname*<br>• -dns61 *IPv6_primary_dns_ip_address*<br>• -dns62 *IPv6_secondary_dns_ip_address*<br>• -dns63 *IPv6_tertiary_dns_ip_1address* | `dhcpinfo -eth0` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Display Ethernet channel 0 DHCP configuration for standbyCMM** | If the IP configuration for the standby CMM eth0 is assigned by a DHCP server, the configuration that is assigned by the DHCP server and DHCP server information is displayed. If the IP configuration for eth0 is *not* assigned by a DHCP server, an error message is displayed. Possible configuration values returned are:<br>• -server *dhcp_ip_address*<br>• -n *hostname*<br>• -i *ip_address*<br>• -g *gateway_address*<br>• -s *subnet_mask*<br>• -d *domainname*<br>• -dns1 *primary_dns_ip_address*<br>• -dns2 *secondary_dns_ip_address*<br>• -dns3 *tertiary_dns_ip_1address*<br>• -server6 *IPv6_dhcp_ip_address*<br>• -i6 *IPv6_address*<br>• -d6 *IPv6_domainname*<br>• -dns61 *IPv6_primary_dns_ip_address* | `dhcpinfo -eth0 -standby` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 30. dhcpinfo command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | • -dns62 *IPv6_secondary_dns_ip_address*<br>• -dns63 *IPv6_tertiary_dns_ip_1address* | | |
| **Display management network DHCP configuration for all compute node interfaces** | Displays the IPv6 configuration for all interfaces of the specified compute node assigned by a DHCP server. If the IP configuration for a compute node interface is *not* assigned by a DHCP server, an error message is displayed.<br>**Note:** If the CMM and compute nodes are set up to use DHCP and the CMM loses network connectivity, the CMM will attempt to acquire a new IP address when network connectivity is restored. The compute nodes will not attempt to acquire an IP address again; they will continue using their existing IP addresses. If you experience compute node network problems after connectivity between the CMM and network is restored, you might need to reset the system-management processor on each compute node in the chassis (including optional Lenovo XClarity Administrator or Flex System Manager hardware, if it is installed). | `dhcpinfo` | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |

*Table 30. dhcpinfo command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display management network DHCP configuration for specific compute node interface** | If the IPv6 configuration for the specified compute node interface is assigned by a DHCP server, the IPv6 IP address is displayed. If the IP configuration for the specified compute node interface is *not* assigned by a DHCP server, an error message is displayed. | `dhcpinfo` -*interface_label*<br>where *interface_label* is any interface label reported by the compute node that specifies both the interface type and channel number. For example, `eth0` for Ethernet channel 0. Valid interface types include:<br>• `usb` for USB<br>• `eth` for Ethernet<br>Valid interface types for a specific compute node can be seen by running the `dhcpinfo` command with no interface argument. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |
| **Display DHCP configuration for I/O module** | If the IPv6 configuration for the specified I/O module is assigned by a DHCP server, the IPv6 IP address is displayed. If the IPv6 configuration for the I/O module is *not* assigned by a DHCP server, an error message is displayed. | `dhcpinfo` | I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |

**Example:** To display the DHCP server assigned network settings for the compute node in bay 2, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type
`dhcpinfo -T blade[2]`

To display the DHCP server assigned network settings for Ethernet channel 0 of the compute node in bay 2, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type
`dhcpinfo -T blade[2] -eth0`

To display the DHCP server assigned network settings for Ethernet channel 0 of the primary CMM, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type
`dhcpinfo -eth0 -T mm[p]`

To display the DHCP server assigned network settings for Ethernet channel 0 of the standby CMM, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type
`dhcpinfo -eth0 -standby -T mm[p]`

The following example shows the information that is returned from these commands:

```
system> dhcpinfo -T blade[2]

eth0
-i6 2000:1013::45b8:6a2a:ff92:4cd3

usb0
```

```
-i6 ::

system> dhcpinfo -T blade[2] -eth0
-i6 2000:1013::45b8:6a2a:ff92:4cd3

system> dhcpinfo -eth0 -T mm[p]
DHCP is disabled
-server6 fd55:faaf:e1ab:1019:9:37:64:33
-i6 fd55:faaf:e1ab:1019:277d:755d:da17:b127
-d6
-dns61 fd55:faaf:e1ab:1019:9:37:64:33
-dns62 fd55:faaf:e1ab:1019:d143:5ba3:e825:1136
-dns63

system> dhcpinfo -eth0 -standby -T mm[p]
DHCP is disabled
-server6 fd55:faaf:e1ab:1019:9:37:64:33
-i6 fd55:faaf:e1ab:1019:4beb:50a3:ac71:b49f
-d6
-dns61 fd55:faaf:e1ab:1019:9:37:64:33
-dns62 fd55:faaf:e1ab:1019:d143:5ba3:e825:1136
-dns63 ::

system>
```

## displaylog command

This command displays CMM event log entries.

**Notes:**

- See the *Installation and Service Guide* for your Flex System chassis for a complete list of all non-device specific events and recommended actions, sorted by event ID. Device specific event information is in the documentation for the device.
- When the CMM is set to “Secure” security mode, only secure file transfer methods, such as HTTPS and SFTP, can be used for tasks involving file transfer when the CMM is acting as a server. Unsecure file transfer protocols, such as HTTP, FTP, and TFTP, are disabled when the CMM is acting as a server when the security mode is set to “Secure”. Unsecure file transfer protocols remain available for a CMM acting as a client for all commands when the security mode is set to “Secure”.
- For information about how to specify a URL for file transfer, see “Specifying a URL for file transfer” on page 29.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See “Common errors” on page 407 for a list of error messages that apply to all commands or “displaylog command errors” on page 427 for a list of error messages that are specific to the displaylog command.

*Table 31. displaylog (display CMM event log) command*

| Function | What it does | Command | **Target** *(see paths in "*Command targets*" on page 6)* |
|---|---|---|---|
| **Display CMM event log entries** | Displays five entries from the CMM event log. The first time the command is executed, the five most recent log entries are displayed. Each subsequent time the command is issued, the next five entries in the log display. | `displaylog` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Display CMM event log entries (reset counter)** | Resets the counter and displays the first five most recent entries in the CMM event log. | `displaylog -f` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Display log entries with Event ID** | Displays log entries with Event ID.<br>**Note:** An asterisk ( * ) after the Event ID indicates that this is a compute node generated event ID. | `displaylog -e` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Display log entries with their call-home flag** | Displays log entries with their call-home flag. | `displaylog -c` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Display all CMM event log entries** | Displays all entries in the CMM event log. | `displaylog -a` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Display log entries with log sequence number** | Displays log entries with their log sequence number event log.<br>**Note:** An asterisk ( * ) after the event sequence number indicates auxiliary data is available for that entry. This can be viewed using the -aux option. | `displaylog -sn` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 31. displaylog (display CMM event log) command (continued)

| Function | What it does | Command | **Target** *(see paths in "*Command targets*" on page 6)* |
|---|---|---|---|
| **Display log entries with auxiliary data** | Displays log entries with their auxiliary data. | `displaylog -aux` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Display all event log filters** | Displays all filters that can be used to control CMM event log output. | `displaylog -filters` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Display event log entries filtered by date** | Displays CMM event log information that meets the specified date filter criteria.<br>**Notes:**<br>• This command displays the first five most recent entries in the CMM event log that meet the specified filter criteria. Adding the -a option to the command displays all entries that meet the specified filter criteria.<br>• If the filter criteria entered does not match the criteria previously specified, this resets the counter and displays the first five most recent log entries that match the specified filter criteria.<br>• The index number displayed for each filtered log entry might not match the index number shown for the same log entry displayed in an unfiltered list. | `displaylog -date` *date_filter*<br>where *date_filter* is a pipe ( \| ) separated list of date filters in mm/dd/yy format. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 31. displaylog (display CMM event log) command (continued)*

| Function | What it does | Command | **Target** *(see paths in* "Command targets" *on page 6)* |
|---|---|---|---|
| **Display event log entries filtered by severity level** | Displays CMM event log information that meets the specified severity level filter criteria.<br>**Notes:**<br>• This command displays the first five most recent entries in the CMM event log that meet the specified filter criteria. Adding the -a option to the command displays all entries that meet the specified filter criteria.<br>• If the filter criteria entered does not match the criteria previously specified, this resets the counter and displays the first five most recent log entries that match the specified filter criteria.<br>• The index number displayed for each filtered log entry might not match the index number shown for the same log entry displayed in an unfiltered list. | `displaylog -sev` *severity_filter*<br>where *severity_filter* is a pipe (`\|`) separated list of severity filters:<br>• `I` (information)<br>• `E` (error)<br>• `W` (warning) | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Display event log entries filtered by every flag except the one specified** | Displays CMM log information that is stored in logs other than the specified log.<br>**Notes:**<br>• This command displays the first five most recent entries in the CMM event log that meet the specified filter criteria. Adding the -a option to the command displays all entries that meet the specified filter criteria.<br>• If the filter criteria entered does not match the criteria previously specified, this resets the counter and displays the first five most recent log entries that match the specified filter criteria.<br>• The index number displayed for each filtered log entry might not match the index number shown for the same log entry displayed in an unfiltered list. | `displaylog -src !` *filter_out*<br>where *filter_out* is the category of event log entries that is not to be displayed. Use the `displaylog -filters` command to discover excludable event log categories. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 31. displaylog (display CMM event log) command (continued)

| Function | What it does | Command | Target (see paths in "Command targets" on page 6) |
|---|---|---|---|
| **Display audit log entries filtered by source** | Displays CMM audit log information that meets the specified source filter criteria.<br>**Notes:**<br>- This command displays the first five most recent entries in the CMM event log that meet the specified filter criteria. Adding the -a option to the command displays all entries that meet the specified filter criteria.<br>- If the filter criteria entered does not match the criteria previously specified, this resets the counter and displays the first five most recent log entries that match the specified filter criteria.<br>- The index number displayed for each filtered log entry might not match the index number shown for the same log entry displayed in an unfiltered list. | `displaylog -src` *source_filter*<br>where *source_filter* is a pipe ( \| ) separated list of source filters, such as `Audit` for the audit log. To specify a range of compute nodes as the source, use a hyphen ( - ), as follows: `Blade_01-08` . | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Display log entries filtered by call-home flag** | Displays log entries that meet the specified call-home events filter criteria.<br>**Notes:**<br>- This command displays the five most recent entries in the CMM event log that meet the specified filter criteria. Adding the -a option to the command displays all entries that meet the specified filter criteria.<br>- If the filter criteria entered does not match the criteria previously specified, this resets the counter and displays the first five most recent log entries that match the specified filter criteria.<br>- The index number displayed for each filtered log entry might not match the index number shown for the same log entry displayed in an unfiltered list. | `displaylog -ch` *option*<br>where *option* are:<br>- `C` (call home)<br>- `N` (non-serviceable)<br>- `S` (serviceable) | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Display the state of the log state event option** | Displays the state (enabled or disabled) of the log state event option, which generates an event when the event log becomes 75% or 100% full. | `displaylog -lse` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 31. displaylog (display CMM event log) command (continued)*

| Function | What it does | Command | **Target** *(see paths in "*Command targets*" on page 6)* |
|---|---|---|---|
| **Enable / disable monitoring of event log state** | Enables or disables the monitoring of the event log state to generate an event when the log becomes 75% or 100% full.<br>**Note:** The displaylog -lse command must be run exclusive of other log-reading command options (-f, -a, -filters, -date, -sev, - src, -i, and -l). | `displaylog -lse` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis log management<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Save event log** | Saves the CMM event log to the specified location. | `displaylog -u` *URL*<br>where *URL* is the fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the event log is to be saved. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

**Example:**

To display all log entries generated by the primary CMM in bay 1 other than those in the audit log, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type
`displaylog -src !Audit -T mm[p]`

To display audit log entries generated by the primary CMM in bay 1, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type
`displaylog -src Audit -T mm[p]`

The following example shows the information that is returned from these commands:

```
system> displaylog -src !Audit -T mm[p]
1       I       SERVPROC   08/04/11    14:18:06     Recovery Event log full
2       I       SERVPROC   08/04/11    14:18:06     Alarm Manager removed a MNR
                                                     alert during recovery of Event
                                                     log full
(There are no more entries in the event log.)
system> displaylog -src audit -T mm[p]
1       I       Audit      08/04/11    14:28:38     Remote logoff successful for
                                                     user 'spdev'from Telnet at
                                                     IP 9.44.124.157
2       I       Audit      08/04/11    14:28:18     Remote login successful for
                                                     user 'spdev' from Telnet at
                                                     IP 9.44.124.157
3       I       Audit      08/04/11    14:18:15     Audit log cleared by 'spdev'.
(There are no more entries in the event log.)
system>
```

## displaysd command

This command captures service data for users to download.

Service information for the CMMs includes Lenovo Flex System component VPD, the CMM event log, connection status, and self-test results. If multiple user interface sessions issue the displaysd command, the commands will be processed in the order that they are received. Some types of service information are displayed for only the primary CMM.

**Notes:**

- When the CMM is set to "Secure" security mode, only secure file transfer methods, such as HTTPS and SFTP, can be used for tasks involving file transfer when the CMM is acting as a server. Unsecure file transfer protocols, such as HTTP, FTP, and TFTP, are disabled when the CMM is acting as a server when the security mode is set to "Secure". Unsecure file transfer protocols remain available for a CMM acting as a client for all commands when the security mode is set to "Secure".
- For information about how to specify a URL for file transfer, see "Specifying a URL for file transfer" on page 29.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "displaysd command errors" on page 429 for a list of error messages that are specific to the displaysd command.

*Table 32. displaysd command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display CMM connection and self-test status** | Displays connection status and latest self-test results for the primary CMM.<br>**Note:** The displaysd -mmstat command must be run exclusive of other command options | `displaysd -mmstat` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Save service information (with warnings)** | Saves service information from primary CMM to the specified location, displaying any warnings about standby CMM that might occur. | `displaysd -u` *URL*<br>where *URL* is the fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the service information is to be saved. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Save service information (override warnings)** | Saves service information from primary CMM to the specified location, overriding warnings about standby CMM. | `displaysd -u` *URL* `-o`<br>where *URL* is the fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the service information is to be saved. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

**Example:** To display connection status and latest self-test results for the primary CMM in bay 1, while the chassis is set as the persistent command environment, at the system> prompt, type:

```
displaysd -mmstat -T system:mm[1]
```

The following example shows the information that is returned from this command:

```
system> displaysd -mmstat -T system:mm[1]

Basic Information for MM Bay 1
Role                      : Primary
Name                      : SN#Y031BG23200P
MAC Address               : 5C:F3:FC:25:E7:C9
UUID                      : 32E9 70CC 6A0D 11E1 A398 C154 23AE AA09
Serial no.                : Y031BG23200P
Build ID                  : 2PET516

Connectivity Status for MM Bay 1
Last Update               : 01/16/14 20:11:21
Node 01                   : Communicating
Node 03                   : Communicating
Node 05                   : Communicating
Node 07                   : Communicating
Node 09                   : Communicating
Node 10 - 01               : Communicating
Node 10 - 02               : Communicating
I/O Module 1               : Communicating
I/O Module 2               : Not Installed
I/O Module 3               : Communicating
I/O Module 4               : Communicating
Rear LED Card              : Communicating
Power Supply 1             : Communicating
Power Supply 2             : Communicating
Power Supply 3             : Communicating
Power Supply 4             : Communicating
Power Supply 5             : Communicating
Power Supply 6             : Communicating
Chassis Cooling Device 1   : Communicating
Chassis Cooling Device 2   : Communicating
Chassis Cooling Device 3   : Communicating
Chassis Cooling Device 4   : Communicating
Chassis Cooling Device 5   : Communicating
Chassis Cooling Device 6   : Communicating
Chassis Cooling Device 7   : Communicating
Chassis Cooling Device 8   : Communicating
Chassis Cooling Device 9   : Communicating
Chassis Cooling Device 10  : Communicating
Fan Mux 1                  : Communicating
Fan Mux 2                  : Communicating
Alternate MM              : Communicating

BIST Results for MM Bay 1
Last Update               : 01/16/14 20:11:21
Real-time Clock           : Passed
Local Management Bus       : Passed
Primary Filesystem        : Passed
Secondary Filesystem      : Passed
Boot Loader (UBOOT)        : Passed
Ethernet Port (eth0)       : Passed
External Management Bus    : Passed
Internal Ethernet Switch   : Passed
Primary kernel          : Passed
Backup kernel           : Passed
Physical Network Link   : Passed
Logical Network Link    : Passed
```

```
MM Bay 2 does not exist
system>
```

**Notes:**

- In this example, node 10 indicates the substructure that is present for logical node groupings and storage expansion enclosures.
- If a large amount of service information is available, display could exceed the capacity of your command-prompt window, resulting in loss of information displayed at the start of the data set. If this happens, you will need to clear the CMM event log to reduce the amount of information being captured.

## dns command

This command configures and displays the CMM DNS settings.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "dns command errors" on page 430 for a list of error messages that are specific to the dns command.

*Table 33. dns command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display DNS configuration of CMM** | Displays the current DNS configuration of the CMM. Possible return values are:<br>• enabled<br>• disabled<br>• -i1 *IPv4_first_ip_address*<br>• -i2 *IPv4_second_ip_address*<br>• -i3 *IPv4_third_ip_address*<br>• -i61 *IPv6_first_ip_address*<br>• -i62 *IPv6_second_ip_address*<br>• -i63 *IPv6_third_ip_address*<br>• -ddns *dynamic_DNS_state* (enabled/disabled)<br>• -p *DNS_server_priority* (ipv4/ ipv6) | `dns` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[x]`<br>where *x* is the primary CMM bay number. |
| **DNS - enable** | Enables the CMM DNS configuration.<br>**Notes:**<br>• At least one IP address must be non-zero to enable DNS.<br>• Any additional DNS servers are added to the top of the search list. Hostname lookup is done on these servers before a DNS server that is assigned automatically by a DHCP server. | `dns -on`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[x]`<br>where *x* is the primary CMM bay number. |

*Table 33. dns command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **DNS - disable** | Disables the CMM DNS configuration.<br>**Notes:**<br>• DNS lookup is always enabled.<br>• When DHCP is in use, other DNS addresses might be assigned automatically by the DHCP server. | `dns -off`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Dynamic DNS - enable / disable** | Enables or disables dynamic DNS for the CMM. | `dns -ddns` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **DNS first IPv4 IP address - set** | Sets the first IPv4 IP address.<br>**Notes:**<br>• At least one IP address must be non-zero to enable DNS.<br>• Any additional DNS servers are added to the top of the search list. Hostname lookup is done on these servers before a DNS server that is assigned automatically by a DHCP server. | `dns -i1` *ip_address*<br>where *ip_address* is the first IP address in dotted decimal IP address format.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 33. dns command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **DNS second IPv4 IP address - set** | Sets the second IPv4 IP address.<br>**Notes:**<br>- At least one IP address must be non-zero to enable DNS.<br>- Any additional DNS servers are added to the top of the search list. Hostname lookup is done on these servers before a DNS server that is assigned automatically by a DHCP server. | `dns -i2` *ip_address*<br>where *ip_address* is the second IP address in dotted decimal IP address format.<br>This command can only be run by users who have one or more of the following command authorities:<br>- Supervisor<br>- Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **DNS third IPv4 IP address - set** | Sets the third IPv4 IP address.<br>**Notes:**<br>- At least one IP address must be non-zero to enable DNS.<br>- Any additional DNS servers are added to the top of the search list. Hostname lookup is done on these servers before a DNS server that is assigned automatically by a DHCP server. | `dns -i3` *ip_address*<br>where *ip_address* is the third IP address in dotted decimal IP address format.<br>This command can only be run by users who have one or more of the following command authorities:<br>- Supervisor<br>- Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **DNS first IPv6 IP address - set** | Sets the first IPv6 IP address.<br>**Notes:**<br>- At least one IP address must be non-zero to enable DNS.<br>- Any additional DNS servers are added to the top of the search list. Hostname lookup is done on these servers before a DNS server that is assigned automatically by a DHCP server. | `dns -i61` *ip_address*<br>where *ip_address* is the first IP address in IPv6 format.<br>This command can only be run by users who have one or more of the following command authorities:<br>- Supervisor<br>- Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 33. dns command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **DNS second IPv6 IP address - set** | Sets the second IPv6 IP address.<br>**Notes:**<br>- At least one IP address must be non-zero to enable DNS.<br>- Any additional DNS servers are added to the top of the search list. Hostname lookup is done on these servers before a DNS server that is assigned automatically by a DHCP server. | `dns -i62` *ip_address*<br>where *ip_address* is the second IP address in IPv6 format.<br>This command can only be run by users who have one or more of the following command authorities:<br>- Supervisor<br>- Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **DNS third IPv6 IP address - set** | Sets the third IPv6 IP address.<br>**Notes:**<br>- At least one IP address must be non-zero to enable DNS.<br>- Any additional DNS servers are added to the top of the search list. Hostname lookup is done on these servers before a DNS server that is assigned automatically by a DHCP server. | `dns -i63` *ip_address*<br>where *ip_address* is the third IP address in IPv6 format.<br>This command can only be run by users who have one or more of the following command authorities:<br>- Supervisor<br>- Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **DNS server priority - set** | Sets the DNS server priority for the CMM to IPv4 or IPv6.. | `dns -p` *priority*<br>where *priority* is `ipv4` or `ipv6` .<br>This command can only be run by users who have one or more of the following command authorities:<br>- Supervisor<br>- Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

**Example:** To set the first IP address of the CMM DNS server to 192.168.70.29 and enable DNS on the primary CMM that does not have IPv6 support, while the primary CMM in bay 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
dns -i1 192.168.70.29 -on
```

To display the DNS status of the primary CMM, while primary CMM in bay 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
dns
```

The following example shows the information that is returned from these two commands:

```
system:mm[1]> dns -i1 192.168.70.29 -on
system:mm[1]> dns
Enabled
-i1 192.168.70.29
-i2 0.0.0.0
-i3 0.0.0.0
system:mm[1]>
```

To display the DNS status of a primary CMM that supports IPv6, while CMM 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type
`dns`

The following example shows the information that is returned from this command:

```
system:mm[1]> dns
Enabled
Enabled
-i1 192.168.70.230
-i2 0.0.0.0
-i3 0.0.0.0
-i61 2002:1013::211:25ff:fec3:227d
-i62 ::
-i63 ::
-ddns disabled
-p ipv4
system:mm[1]>
```

## env command

This command sets the persistent environment for commands that are entered during the remainder of the current session.

The persistent command environment is indicated by the command prompt. When you start the command-line interface, the persistent command environment is the Lenovo Flex System chassis, denoted as `system` by the command prompt. You can target a single command to an environment other than the one that is set as the default by adding a `-T` option to the command that includes a valid target destination (see "Command targets" on page 6 for information). Target environments can be specified using the full path name, or using a partial path name based on the persistent command environment. Full path names always begin with `system`. The levels in a path name are divided by using a colon ( : ).

See "Command targets" on page 6 for a list of Lenovo Flex System components, command targets, command target paths, and the command targeting hierarchy that is supported by the env command. Target names have been selected to maintain scripting compatibility with other Lenovo systems.

**Note:** To see installed targets for your Lenovo Flex System chassis, use the "list command" on page 224.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "env command errors" on page 431 for a list of error messages that are specific to the env command.

*Table 34. env command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set Lenovo Flex System chassis as command target** | Sets the Lenovo Flex System chassis as the persistent target for commands during the current session. This is the persistent command environment you are in at the beginning of each command-line interface session, indicated by the `system>` prompt. | `env`<br>`env -T system` | The env command can be directed to any installed device. |
| **Set CMM as command target** | Sets the CMM as the persistent target for commands during the current session. | `env -T system:mm` [*x*]<br>where *x* is the bay (1 or 2) that identifies the CMM. | The env command can be directed to any installed device, in this case<br>`mm[`*x*`]`<br>where *x* is the CMM bay number. |
| **Set primary CMM as command target** | Sets the primary CMM as the persistent target for commands during the current session. | `env -T system:mm[p]`<br>`env -T system:mm[P]` | The env command can be directed to any installed device, in this case<br>`mm[p]`<br>`mm[P]` |
| **Set standby CMM as command target** | Sets the standby CMM as the persistent target for commands during the current session. | `env -T system:mm[s]`<br>`env -T system:mm[S]` | The env command can be directed to any installed device, in this case<br>`mm[s]`<br>`mm[S]` |
| **Set compute node as command target** | Sets the specified compute node as the persistent target for commands during the current session. | `env -T system:blade` [*x*]<br>where *x* is the node bay that identifies the compute node. A compute node that occupies more than one node bay is identified by the lowest bay number that it occupies. | The env command can be directed to any installed device, in this case<br>`blade[`*x*`]`<br>where *x* is the node bay that identifies the compute node. |
| **Set logical node grouping as command target** | Sets the logical node grouping as the persistent target for commands during the current session. | `env -T system:bladegroup` [*x*]<br>where *x* is the node bay that identifies the logical node grouping. A logical node grouping that occupies more than one node bay is identified by the lowest bay number that it occupies. | The env command can be directed to any installed device, in this case<br>`bladegroup[`*x*`]`<br>where *x* is the node bay that identifies the logical node grouping. |

*Table 34. env command (continued)*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set compute node in logical node grouping as command target** | Sets the specified compute node in a logical node grouping as the persistent target for commands during the current session.<br>**Note:** When a compute node is part of a logical node grouping, syntax for compute node sub-components is of the form: `env -T system: bladegroup[`*x*`]: blade[`*y*`]:` *comp*, as discussed in Set compute node sub-component as command target | `env -T system: bladegroup[`*x*`]: blade[`*y*`]`<br>where:<br>• *x* is the node bay that identifies the logical node grouping. A logical node grouping that occupies more than one node bay is identified by the lowest bay number that it occupies.<br>• *y* is the identifier for the compute node in the logical node grouping. | The env command can be directed to any installed device, in this case `bladegroup[`*x*`]: blade[`*y*`]`<br>where:<br>• *x* is the node bay that identifies the logical node grouping. A logical node grouping that occupies more than one node bay is identified by the lowest bay number that it occupies.<br>• *y* is the identifier for the compute node in the logical node grouping. |
| **Set compute node sub-component as command target** | Sets the specified sub-component on the specified compute node as the persistent target for commands during the current session. Valid sub-components are:<br>• Node system-management processor<br>• Expansion adapter<br>• Add-in card<br>• Add-in card PCI-Express module<br>• Microprocessor<br>• Expansion node<br>• High-speed expansion card<br>• Memory<br>• Flash DIMM storage (Lenovo eXFlash Storage DIMM)<br>• Storage backplane<br>• Alarm panel | `env -T system:blade [`*x*`]:` *comp*<br>where *x* is the node bay that identifies the compute node on which the sub-component is installed. A compute node that occupies more than one node bay is identified by the lowest bay number that it occupies.<br><br>where *comp* is the sub-component:<br>• `sp` for node system-management processor<br>• `exp [`*x*`]` for expansion adapter (where *x* identifies the expansion adapter)<br>• `cpu [`*x*`]` for microprocessor (where *x* identifies the microprocessor)<br>• `addin [`*x*`]` for add-in card (where *x* identifies the add-in card)<br>• `pciexpress [`*x*`]` for add-in card PCI-Express module (where *x* identifies the PCI-Express module) | The env command can be directed to any installed device, in this case `blade[`*x*`]:`*comp*<br><br>where *x* is the node bay that identifies the compute node on which the sub-component is installed.<br><br>where *comp* is the sub-component:<br>• `sp` for node system-management processor<br>• `exp [`*x*`]` for expansion adapter (where *x* identifies the expansion adapter)<br>• `cpu [`*x*`]` for microprocessor (where *x* identifies the microprocessor)<br>• `addin [`*x*`]` for add-in card (where *x* identifies the add-in card)<br>• `pciexpress [`*x*`]` for add-in card PCI-Express module |

*Table 34. env command (continued)*

| **Function** | **What it does** | **Command** | **Target** *(see paths in* "Command targets" *on page 6)* |
|---|---|---|---|
| | | • `stgbkplane` [*x*] for storage backplane card (where *x* identifies the storage backplane)<br>• `be` [*x*] for expansion node (where *x* identifies the expansion node)<br>• `hsec` [*x*] for high-speed expansion card (where *x* identifies the high-speed expansion card)<br>• `memory` [*x*] for memory (where *x* identifies the memory module)<br>• `flashdimm` [*x*] for flash DIMM (where *x* identifies the flash DIMM storage module)<br>*(continued on next page)* | (where *x* identifies the PCI-Express module)<br>• `be` [*x*] for expansion node (where *x* identifies the expansion node)<br>• `stgbkplane` [*x*] for add-in card (where *x* identifies the storage backplane)<br>• `hsec` [*x*] for high-speed expansion card (where *x* identifies the high-speed expansion card)<br>• `memory` [*x*] for memory (where *x* identifies the memory module)<br>*(continued on next page)* |
| **Set compute node sub-component as command target** *(continued)* | | • `mgmtcrd` [*x*] for management card (where *x* identifies the management card)<br>• `tap` [*x*] for alarm panel (where *x* identifies the alarm panel) | • `flashdimm` [*x*] for flash DIMM (where *x* identifies the flash DIMM storage module)<br>• `mgmtcrd` [*x*] for management card (where *x* identifies the management card)<br>• `tap` [*x*] for alarm panel (where *x* identifies the alarm panel) |
| **Set I/O module as command target** | Sets the specified I/O module as the persistent target for commands during the current session. | `env -T system:switch` [*x*]<br>where *x* is the I/O bay where the I/O module is installed. | The env command can be directed to any installed device, in this case<br>`switch`[*x*]<br>where *x* is the I/O bay where the I/O module is installed. |

*Table 34. env command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set power supply as command target** | Sets the specified power supply as the persistent target for commands during the current session. | `env -T system:power [x]`<br>where *x* is the power supply bay where the power supply is installed. | The env command can be directed to any installed device, in this case<br>`power[x]`<br>where *x* is the power supply bay where the power supply is installed. |
| **Set fan logic module as command target** | Sets the specified fan logic module as the persistent target for commands during the current session. | `env -T system:fanmux [x]`<br>where *x* is the bay where the fan logic module is installed. | The env command can be directed to any installed device, in this case<br>`fanmux[x]`<br>where *x* is the bay where the fan logic module is installed. |
| **Set fan module as command target** | Sets the specified fan module module as the persistent target for commands during the current session. | `env -T system:blower [x]`<br>where *x* is the fan module bay where the fan module is installed. | The env command can be directed to any installed device, in this case<br>`blower[x]`<br>where *x* is the fan module bay where the fan module is installed. |
| **Set rear LED card as command target** | Sets the rear LED card as the persistent target for commands during the current session. | `env -T system:mt [x]`<br>where *x* is the rear LED card. | The env command can be directed to any installed device, in this case<br>`mt[x]`<br>where *x* is the rear LED card. |
| **Set storage expansion enclosure as command target** | Sets the storage expansion enclosure as the persistent target for commands during the current session. | `env -T system: bladeenclosure [x]`<br>where *x* is the storage-expansion-enclosure bay that identifies the storage expansion enclosure. A storage expansion enclosure that occupies more than one node bay is identified by the lowest bay number that it occupies. | The env command can be directed to any installed device, in this case<br>`bladeenclosure[x]`<br>where *x* is the node bay that identifies the storage expansion enclosure. |

**Example:** To set the persistent target of commands to the system-management processor on the compute node in node bay 5, while the Lenovo Flex System chassis is set as the default command target, at the `system>` prompt, type

```
env -T system:blade[5]:sp
```

The following example shows the information that is returned:

```
system> env -T system:blade[5]:sp
OK
system:blade[5]:sp>
```

To set the persistent target of commands to the system-management processor on the compute node in node bay 5, while the Lenovo Flex System chassis is set as the default command target, at the `system>` prompt, you can also type

```
env -T blade[5]:sp
```

The following example shows the information that is returned:

```
system> env -T blade[5]:sp
OK
system:blade[5]:sp>
```

To issue the reset command on the compute node in node bay 5, while the CMM is set as the default command target, at the `system:mm[x]>` prompt, type

```
reset -T system:blade[5]
```

## ethoverusb command

This command sets and displays the setting for the Ethernet-over-USB command interface of a compute node system-management processor, for compute nodes that support this feature.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See “Common errors” on page 407 for a list of error messages that apply to all commands or “ethoverusb command errors” on page 431 for a list of error messages that are specific to the ethoverusb command.

*Table 35. ethoverusb command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display compute node Ethernet-over-USB setting** | Displays the Ethernet-over-USB command interface setting for the system-management processor of the specified compute node.<br>**Note:** This command will execute only on compute nodes that support an Ethernet-over-USB command interface for the node system-management processor. | `ethoverusb` | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |
| **Set compute node Ethernet-over-USB setting** | Enables or disables the Ethernet-over-USB command interface setting for the system-management processor of the specified compute node.<br>**Notes:**<br>• This command will execute only on compute nodes that support an Ethernet-over-USB command interface for the node system-management processor.<br>• You cannot update the firmware for a compute node while the LAN over USB interface is disabled. Before updating the firmware, you must re-enable the interface. After updating the firmware, you can disable the interface again. | `ethoverusb -s` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade administration<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |

**Example:** To view the Ethernet-over-USB command interface setting for the system-management processor of the compute node in bay 11, while this compute node is set as the persistent command environment, at the `system:blade[11]>` prompt, type

```
ethoverusb
```

To disable the Ethernet-over-USB command interface setting for the system-management processor of the compute node in bay 11, while this compute node is set as the persistent command environment, at the `system:blade[11]>` prompt, type

```
ethoverusb -s disabled
```

The following example shows the information that is returned from these commands:

```
system:blade[11]> ethoverusb
-s enabled
system:blade[11]> ethoverusb -s disabled
Notice: This operation may take a short while to complete. Please view the
status to determine when the operation has completed.
OK
system:blade[11]> ethoverusb
-s disabled
system:blade[11]>
```

## events command

This command manages the Call Home events exclusion list for the CMM.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See “Common errors” on page 407 for a list of error messages that apply to all commands or “events command errors” on page 431 for a list of error messages that are specific to the events command.

*Table 36. events command*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display Call Home events list and free space** | Displays a list of Call Home event IDs that will not be reported by the Call Home feature, and how many more events can be added to this Call Home events exclusion list. This Call Home exclusion list allows a maximum of 20 events. | `events -che`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>• Chassis log management<br>• Chassis administration<br>• Chassis configuration<br>• Blade administration<br>• Blade configuration<br>• Blade remote presence<br>• I/O module administration<br>• I/O module configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Add a Call Home event to the Call Home Exclusion list** | Adds a Call Home event to the Call Home exclusion list. Events on this list are specified by an event ID, and are not included in the Call Home reports.<br>**Note:** The Service Advisor terms and conditions must first be accepted, or the Automated FTP/TFTP Report of Service Data must be enabled before using this command. | `events -che -add` *event_ID*<br>where *event_ID* is an eight-digit hexadecimal number with an optional prefix of 0x or 0X.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Remove a Call Home event from the Call Home Exclusion list** | Removes a Call Home event from the Call Home exclusion list. Events removed from this list are included in the Call Home reports.<br>**Note:** The Service Advisor terms and conditions must first be accepted, or the Automated FTP/TFTP Report of Service Data must be enabled before using this command. | `events -che -rm` *event_ID*<br>where *event_ID* is<br>• an eight-digit hexadecimal number with an optional prefix of 0x or 0X to remove a single Call Home event<br>• `all` to remove all the Call Home events from the exclusion list<br>This command can only be run by users who have one or more of the | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 36. events command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | | following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | |

**Example:** To view the Call Home exclusion list and the number of remaining events can be added to the list, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system:>` prompt, type

```
events -T mm[p] -che
```

To add Call Home event number 0x00020003 to the Call Home exclusion list, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
events -T mm[p] -che -add 0x00020003
```

To remove Call Home event number 0x00020001 from the Call Home exclusion list, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
events -T mm[p] -che -rm 0x00020001
```

The following example shows the information that is returned from these commands:

```
system> events -T mm[p] -che
A maximum of 20 events can be added to this exclusion list, currently
18 more events can be added.
Call Home Exclusion List is illustrated as follows:
Index        Event ID
 1           0x00020001
 2           0x00020002
system> events -T mm[p] -che -add 0x00020003
OK
system> events -T mm[p] -che
A maximum of 20 events can be added to this exclusion list, currently
17 more events can be added.
Call Home Exclusion List is illustrated as follows:
Index        Event ID
 1           0x00020001
 2           0x00020002
 3           0x00020003
system> events -T mm[p] -che -rm 0x00020001
OK
system> events -T mm[p] -che
A maximum of 20 events can be added to this exclusion list, currently
18 more events can be added.
Call Home Exclusion List is illustrated as follows:
Index        Event ID
 1           0x00020002
 2           0x00020003
system>
```

## exit command

This command exits the command-line interface, terminating the current session.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "exit command errors" on page 432 for a list of error messages that are specific to the exit command.

*Table 37. exit command*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Exit CLI session** | Terminates the current command-line interface session. | `exit`<br>**Note:** You can also use the Ctrl-D key combination to end the current session and exit the command-line interface. | Any installed device. |

**Example:** To terminate the current command-line interface session, type

```
exit
```

## files command

This command manages files uploaded to the CMM.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "files command errors" on page 432 for a list of error messages that are specific to the files command.

*Table 38. files command*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display file list and free space** | Displays a list of files and space remaining in the CMM file system. | `files` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Delete file** | Deletes a file from the CMM file system.<br>**Note:** This command can only be used to delete files: it will not delete directories. | `files -d` *filename*<br>where *filename* is a valid, existing filename of less than 256 characters in length.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis administration<br>• Chassis configuration<br>• Blade administration<br>• Blade configuration<br>• I/O module administration<br>• I/O module configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

**Example:** To view the files and remaining space in the primary CMM file system, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type
`files -T mm[p]`

To delete the file `tftproot/tftp_file.pkt` from the primary CMM file system, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type
`files -d tftproot/tftp_file.pkt -T mm[p]`

The following example shows the information that is returned from these commands:

```
system> files -T mm[p]
     12288 Thu Jan 05 13:28:23 2015 lost+found/
      1024 Thu Jul 06 19:32:51 2015 tftproot/
      1024 Thu Jul 06 19:34:15 2015 tftproot/test/
      1024 Thu Jul 06 19:34:15 2015 tftproot/test/test2/
         0 Sat Aug 19 09:22:02 2015 tftproot/tftp_file.pkt
         0 Sun Oct 01 07:57:19 2015 tftproot/.Do_not_delete_this_directory
         0 Tue Dec 15 11:07:19 2015 test
         0 Thu Apr 13 23:45:40 2015 bob.pkt
      1024 Tue Feb 02 15:29:17 2015 pubkeys/
       426 Tue Feb 02 15:29:17 2015 pubkeys/ssh_key.pub
      5652 Fri May 12 00:56:36 2015 asm.cfg
```

```
Total space:   73108480 bytes
Used:             24576 bytes
Available:     73083904 bytes
system> files -d tftproot/tftp_file.pkt -T mm[p]
OK
system>
```

## fod command

This command displays licensing information for optional Lenovo Flex SystemCMM and I/O module Features on Demand features.

You can purchase activation keys to activate the Features on Demand features for your CMM and I/O modules, if your I/O modules support these features. For information about Features on Demand, see https://fod.lenovo.com/lkms.

**Note:** The CMM fod command does not support activation of Features on Demand features for compute nodes. If an optional management device, such as the Lenovo XClarity Administrator or Flex System Manager management server, is installed in the Lenovo Flex System chassis, you can activate the Features on Demand features for compute node firmware using the management device program. Depending on your compute node type, other methods are available for activating Features on Demand features for compute nodes. See the documentation for your compute node for information.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "fod command errors" on page 433 for a list of error messages that are specific to the fod command.

*Table 39. fod command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display feature licenses** | Displays a list of optional Features on Demand licenses for the specified command target.<br>**Note:** The license expiration dates and times are in GMT. | `fod` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number.<br>I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |

**Example:** To view the feature license information for the primary CMM in bay 1, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type
`fod -T mm[p]`

The following example shows the information that is returned from this command:

```
system> fod -T mm[p]
Flex System Manager License
    Index: 2
    Status: Validate Elsewhere
    Description: SYSTEM X FEATURE ON DEMAND ACTIVATION KEY
    Size: 428 bytes
    System: Flex System Manager
    Identifier: MTSN 872123DVG73
    Feature: Flex System Manager License
    Feature Type: 000b
    Activation Expiration: Thu Sep 10 05:29:59 2015
    Validation: SHA-1 RSA 2048
system>
```

## fruactlog command

This command displays a summary of the hardware activity for modules installed in the Lenovo Flex System chassis.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "fruactlog command errors" on page 433 for a list of error messages that are specific to the fruactlog command.

*Table 40. fruactlog command*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display chassis activity summary** | Displays a list of hardware activity for chassis modules, along with their VPD information. | `fruactlog` | Lenovo Flex System chassis:<br>`system` |

**Example:** To view the list of chassis module activity and VPD information, while the Lenovo Flex System chassis is set as the default command target, at the `system>` prompt, type
`fruactlog`

The following example shows the information that is returned from this command. Only partial results are shown, since the full results returned when running this command on a functional chassis are lengthily.

```
system> fruactlog

Component: system:bladeenclosure[7]:blade[2]
Name: PRODUCT DESCRIPTION STORAGE ITE
Part Number: 90Y7692
Serial Number: YM11BG22H01X
Manufacturer ID: Lenovo
Time/Date: 09/28/12, 16:24:00
Action: Inserted

Component: system:switch[2]
Name: EN4093 10Gb Ethernet Switch
Part Number: 49Y4273
Serial Number: Y250VT16Y258
Manufacturer ID: Lenovo
Time/Date: 09/25/12, 13:59:37
Action: Inserted

Component: system:power[1]
Name: Power Supply
Part Number: 69Y5806
Serial Number: ZK128116T034
Manufacturer ID: Lenovo
```

```
Time/Date: 09/25/12, 13:59:07
Action: Inserted

.
.
.

system>
```

## fsmcm command

This command disables centralized user account management from an optional management device, such as the Lenovo XClarity Administrator or Flex System Manager management software, allowing use of local CMM user accounts.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See “Common errors” on page 407 for a list of error messages that apply to all commands or “fsmcm command errors” on page 434 for a list of error messages that are specific to the fsmcm command.

*Table 41. fsmcm (disable centralized account management) command*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Disable centralized user account management** | Disables centralized account management, allowing use of local CMM user accounts.<br>**Notes:**<br>• Centralized user account management is enabled by the optional management device software.<br>• When centralized user account management is enabled by the optional management device software:<br>– All CMM user accounts are disabled, except for the RECOVERY_ID account that unlocks the CMM and issues commands to configure the CMM LDAP client.<br>– Users logged in to the CMM web interface and CLI are logged out when their user accounts are disabled.<br>• When running the `fsmcm -off` command using the management device software created recovery account (RECOVERY_ID):<br>– The CMM CLI session for the RECOVERY_ID user account terminates. You will need to use an existing CMM user account to access the CMM web interface or CLI, until centralized user management is restored.<br>– The RECOVERY_ID user account is deleted.<br>– Management of compute node IPMI and SNMPv3 user accounts by the CMM is disabled. This function can be enabled using the `users -am enabled` command (see "users command" on page 372).<br>• See the Lenovo XClarity Administrator or Flex System Manager documentation for information about accessing the CMM after centralized user account management is enabled. | `fsmcm -off`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

**Example:** To disable centralized user account management when logged in using the RECOVERY_ID user account, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
fsmcm -off -T mm[p]
```

The following example shows the information that is returned when this command is entered:

```
system> fsmcm -off -T mm[p]
Connection to 192.168.70.125 closed by remote host.
Connection to 192.168.70.125 closed.
```

**Note:** The connection closes when running this command because it terminates the CLI session.

## fuelg command

This command displays power domain information, listing the power supplies that are installed in the Lenovo Flex System chassis and information about power usage. This command also configures policies for power redundancy loss and limiting fan noise during thermal events.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "fuelg command errors" on page 434 for a list of error messages that are specific to the fuelg command.

*Table 42. fuelg command*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display power domain status overview** | Displays health status, total power usage, total dc power available, total ac power in use, thermal response (acoustic mode) settings, total thermal output in BTU/hour, chassis static power limit, and the hot air recirculation detection state.<br>**Note:** The chassis static power limit (-spl) indicates the set value as both a percentage and a wattage, along with the upper and lower wattage values that can be set. | `fuelg` | Lenovo Flex System chassis:<br>`system` |
| **Display compute node power status overview** | Displays the power management and capping setting (on/off) and power management capability for the specified compute node. Depending on the power management capability of the specified compute node, the following information will also display:<br>• CPU duty cycles<br>• Effective and maximum CPU speeds<br>• Power capping value (minimum and maximum)<br>• Maximum, minimum, and average power levels<br>• Time when above data was captured<br>• Power saver mode status (on, off) | `fuelg` | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |

*Table 42. fuelg command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display I/O module power status** | Displays the maximum, minimum, and average power information for the specified I/O module. | `fuelg` | I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |
| **Display fan module power status and temperature** | Displays the maximum power, minimum power, average power, and current temperature information for the specified fan module. | `fuelg` | Fan module:<br>`blower[`*x*`]`<br>where *x* is the fan module bay number. |
| **Display rear LED card temperature** | Displays the minimum, maximum, and average temperature for the specified rear LED card. | `fuelg` | Rear LED card:<br>`mt[`*x*`]`<br>where *x* is the rear LED card. |
| **Display detailed power domain status** | Displays detailed status and usage information for the power domain, including the policy setting for that domain, the maximum power limit, and the power in use. The valid states for components in the domain are:<br>• * - compute node might throttle<br>• C - communication error<br>• D - discovering<br>• Hib - hibernate<br>• NP - module is not present<br>• SB - standby<br>• T - throttled<br>• U - unable to power up<br>**Note:** The Lenovo Flex System chassis has only one power domain. | `fuelg pd` | Lenovo Flex System chassis:<br>`system` |

Table 42. fuelg command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set power domain redundancy loss policy** | Sets how the Lenovo Flex System chassis responds to a condition that could cause a loss of redundant power. | `fuelg pd -pm` *policy*<br>where *policy* is:<br>• `acred` (ac power source redundancy policy)<br>• `acredov` (ac power source redundancy policy, with compute node throttling)<br>• `redwoperf` (power module redundancy, no compute node oversubscription)<br>• `redwperf` (power module redundancy with compute node power throttling)<br>• `nonred` (no power management policy)<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system` |
| **Display power trending for specified time period for power domain** | Displays power trending information, for the selected time interval, for the power domain of the Lenovo Flex System chassis.<br>**Note:** The Lenovo Flex System chassis has only one power domain. | `fuelg pd -pt` *period*<br>where *period* is 1, 6, 12, or 24 hours. | Lenovo Flex System chassis:<br>`system` |

Table 42. fuelg command (continued)

| Function | What it does | Command | Target (see paths in "Command targets" on page 6) |
|---|---|---|---|
| **Display power trending for specified time period** | Displays power trending information for the selected time interval for the specified command target. | `fuelg -pt` *period*<br>where *period* is 1, 6, 12, or 24 hours. | Lenovo Flex System chassis:<br>`system`<br>Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number.<br>I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number.<br>Fan module:<br>`blower[`*x*`]`<br>where *x* is the fan module bay number. |
| **Display thermal trending for specified time period** | Displays thermal trending information (minimum, maximum, and average temperature) for the selected time interval for the specified command target. | `fuelg -tt` *period*<br>where *period* is 1, 6, 12, or 24 hours. | Rear LED card:<br>`mt[`*x*`]`<br>where *x* is the rear LED card.<br>Fan module:<br>`blower[`*x*`]`<br>where *x* is the fan module bay number. |
| **Display exhaustive heat trending information for chassis for specified time period** | Displays exhaustive heat trending information for the chassis for the selected time interval. | `fuelg -ht` *period*<br>where *period* is 1, 6, 12, or 24 hours. | Lenovo Flex System chassis:<br>`system` |

*Table 42. fuelg command (continued)*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set hot air recirculation detection state** | Enables or disables hot air recirculation detection for the Lenovo Flex System chassis. | `fuelg -har` *setting*<br>where a *setting* of:<br>• `disabled` turns off hot air recirculation detection for the chassis.<br>• `enabled` (default) turns on hot air recirculation detection for the chassis.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system` |
| **Set hot air recirculation threshold** | Sets the hot air recirculation threshold, the maximum allowable temperature difference between the input and output sensors, for the specified command target. If this threshold is exceeded, a hot air recirculation event is created in the CMM event log. | `fuelg -hart` *setting*<br>where *setting* is a temperature, between, 5.00 and 9.00 Celsius, that triggers a hot air recirculation event. For example, a value of `6.00` would trigger an event if the output temperature was more than 6.00 degrees greater than the input temperature.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system` |
| **Display air flow trending for specified time period** | Displays chassis air flow trending information, in cubic feet per minute (CFM), for the selected time interval. | `fuelg -aft` *period*<br>where *period* is 1, 6, 12, or 24 hours. | Lenovo Flex System chassis:<br>`system` |

*Table 42. fuelg command (continued)*

| Function | What it does | Command | Target *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Thermal event response** (acoustic mode) | Sets the acoustic mode of Lenovo Flex System chassis fan system response to thermal events.<br>**Notes:** When the CMM is installed in a Lenovo Flex System Carrier-Grade chassis:<br>• Turning on NEBS mode (`fuelg -am on`) turns off acoustic mode (`-am off`).<br>• Setting acoustic mode to a value of 1 through 5 (`-am` *x*, where *x* is 1 though 5) turns off NEBS mode (`fuelg -am off`).<br>• The NEBS (`-nm`) setting overrides the acoustic mode (`-am`) setting if both options are specified at the same time. | `fuelg -am` *setting*<br>where the acoustic-mode *setting* is `off` or a number from 1 to 5, inclusive. A value of `off` disables acoustic mode (fans run at maximum requested speed, providing highest cooling). A value of 1 provides low attenuation (higher cooling). A value of 5 provides highest attenuation (lowest cooling). If you enter a value outside this range, an error will be displayed.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system` |
| **Set NEBS mode for chassis**<br>**Note:** This command option applies only to CMMs installed in a Lenovo Flex System Carrier-Grade chassis. | Enables or disables NEBS (Network Equipment-Building System) mode for a Lenovo Flex System Carrier-Grade chassis.<br>**Notes:**<br>• Turning on NEBS mode (`-am on`) turns off acoustic mode (`fuelg -am off`).<br>• Setting acoustic mode to a value of 1 through 5 (`fuelg -am` *x*, where *x* is 1 though 5) turns off NEBS mode (`-am off`).<br>• The NEBS (`-nm`) setting overrides the acoustic mode (`-am`) setting if both options are specified at the same time. | `fuelg -nm` *setting*<br>where *setting* is `off` or `on`.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system` |

*Table 42. fuelg command (continued)*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set static power limit** | Sets the static power limit value for the Lenovo Flex System chassis.<br>**Note:** To set the static power limit value for the chassis, power management and capping for the chassis must *not* be set to none (`fuelg -pme static` ). | `fuelg -spl` *setting*<br>where *setting* is:<br>• a maximum percentage, between, 0 and 100, of total available power. For example, a value of `80` would set the upper limit of available power to 80 percent of total available power. The percentage selected must fall within the range of available power for the chassis.<br>• a maximum wattage value, indicated by `w`, within the range of total available power. For example, a value of `5000w` would make up to 5000 watts of power available for use by chassis components.<br>Available power for a chassis is displayed by running the `fuelg` command, with no options, on the `system` target.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system` |
| **Set power capping value** | Sets the power capping value for the specified command target that supports this feature.<br>**Notes:**<br>• Setting a power capping value for a compute node, automatically turns on power management and capping for the compute node (`fuelg -pme on` ).<br>• A compute node must be turned on before you can set its power capping value.<br>• When setting `-pcap` to the maximum power limit value for a range, verify that there is sufficient power available in the | `fuelg -pcap` *setting*<br>where *setting* is a numeric wattage value that falls within the range of power capping values displayed when running the `fuelg` command, with no options, on the target.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |

Table 42. fuelg command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | budget, or the setting will be rejected. Use the `fuelg` command with no options to see the amount of power currently allocated.<br>• Reconfiguration of the `fuelg -pcap` value might be required when disabling `fuelg -dps` to make sure that the power allocated for a node is not greater than the maximum power limit allowed. | authority" on page 10 for additional information. | |
| **Power management and capping - enable or disable** | Turns power management and capping for the specified command target on or off.<br>**Notes:**<br>• If power management and capping is set to `static` for a chassis, you must also specify a static power limit value (`fuelg -spl` *value*).<br>• A compute node must be turned on before you can enable power management and capping for it. | `fuelg -pme` *setting*<br>where:<br>• for the chassis target, a *setting* of:<br>– `none` (default) disables power management and capping for the chassis.<br>– `static` enables power management and capping for the chassis.<br>• for a compute node target, a *setting* of:<br>– `off` (default) disables power management and capping for the compute node.<br>– `on` enables power management and capping for the compute node.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system`<br>Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |

*Table 42. fuelg command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Static low power saver mode - enable or disable for compute node** | Turns the static low power saver mode for the specified compute node on or off.<br>**Notes:**<br>• A compute node must be turned on before you can enable power saver mode for it.<br>• Not all compute nodes support the power saver mode. | `fuelg -ps` *setting*<br>where a *setting* of:<br>• `off` (default) disables power saver mode for the compute node.<br>• `on` enables power saver mode for the compute node.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |
| **Dynamic power optimizer - enable or disable for compute node** | Turns dynamic power optimizer for the specified compute node on or off.<br>**Notes:**<br>• A compute node must be turned on before you can enable dynamic power optimizer for it.<br>• Not all compute nodes support the dynamic power optimizer.<br>• When enabling `-dps`, set `fuelg -pcap` to the maximum power limit value for that range so the node receives the full benefit of dynamic power optimizer mode. When setting `fuelg -pcap` to the maximum power limit value for a range, verify that there is sufficient power available in the budget, or the setting will be rejected. Use the `fuelg` command with no options to see the amount of power currently allocated.<br>• When disabling `-dps`, make sure that the configured `fuelg -pcap` value for the node is not greater than the maximum power limit for the `-dps` disabled range. Reconfiguration of the `fuelg -pcap` value might be required to make sure that the power allocated for a node is not greater than the maximum power limit allowed. | `fuelg -dps` *setting*<br>where a *setting* of:<br>• `off` (default) disables dynamic power optimizer for the compute node.<br>• `on` enables dynamic power optimizer for the compute node.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |

*Table 42. fuelg command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Favor performance over power - enable or disable for compute node** | Turns the favor performance over power feature on or off for the specified compute node.<br>**Notes:**<br>• A compute node must be turned on before you can enable the favor performance over power feature for it.<br>• Not all compute nodes support the favor performance over power feature.<br>• This feature can only be active if the dynamic power optimizer is enabled. | `fuelg -fpop` *setting*<br>where a *setting* of:<br>• `off` (default) disables favor performance over power for the compute node.<br>• `on` enables favor performance over power for the compute node.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |

**Example:** To view a power domain status overview, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
fuelg
```

To view the detailed power domain status for the power domain, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
fuelg pd
```

To view Lenovo Flex System chassis power trending information for the past 6 hours, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
fuelg -pt 6
```

To view the power status for the compute node in blade bay 9, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
fuelg -T blade[9]
```

To view thermal trending information for the rear LED card in bay 1, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
fuelg -T mt[1] -tt 1
```

The following examples show the information that is returned from these commands.

```
system> fuelg
Note: All power values are displayed in Watts.

Total DC Power Available: 13725
Total Power In Use:        678 (+/- 0.5%)
Total Thermal Output:      2313 BTU/hour

Power Domain
--------------
Status: Power domain status is good.
```

```
Modules:
 Bay 1:   2745
 Bay 2:   2745
 Bay 3:   2745
 Bay 4:   2745
 Bay 5:   2745
 Bay 6:   2745 (off)
Power Management Policy: Basic Power Management
Power in Use:            596 (+/- 0.5%)
Total Power:           13725
Allocated Power (Max):  3233
Remaining Power:       10492
Power Service: 220 VAC

-am  off
-pme  static
-spl 90 (12489W, min: 3233W, max: 13725W)
-har enabled
-hart 5.00

Component: system
Temp: 23.50 C
Threshold exceeded: No

Component: system:bladegroup[3]:blade[1]
Temp: 23.00 C
Threshold exceeded: No

Component: system:bladegroup[3]:blade[2]
Temp: 23.00 C
Threshold exceeded: No

Component: system:blade[4]
Temp: 22.00 C
Threshold exceeded: No

Component: system:bladeenclosure[7]:blade[1]
Temp: 23.00 C
Threshold exceeded: No

Component: system:bladeenclosure[7]:blade[2]
Temp: 22.00 C
Threshold exceeded: No

Component: system:bladeenclosure[11]:blade[1]
Temp: 29.00 C
Threshold exceeded: Yes

system> fuelg pd
Maximum Power Limit: 13725
Power In Use:          689

                                   Power  -- Allocated Power --
Bay(s)  Module                     State  Current   Max    Min
======  ========================== =====  =======  =====  =====
Chassis Components
        Midplane                    On         38     38     38
     1  Rear LED Card 1             On          2      2      2
Chassis Cooling Devices
     1  Chassis Cooling Device 1    On          9     75     75
     2  Chassis Cooling Device 2    On         11     75     75
     3  Chassis Cooling Device 3       On          12     75     75
     4  Chassis Cooling Device 4       On          11     75     75
     5  Chassis Cooling Device 5       On           7     60     60
     6  Chassis Cooling Device 6       On          11     75     75
     7  Chassis Cooling Device 7       On          11     75     75
     8  Chassis Cooling Device 8       On          10     75     75
     9  Chassis Cooling Device 9       On          10     75     75
    10  Chassis Cooling Device 10      On           6     60     60
Power Module Cooling Devices
     1  PM Cooling Device 1             On          40     40     40
     2  PM Cooling Device 2             On          40     40     40
     3  PM Cooling Device 3             On          40     40     40
     4  PM Cooling Device 4             On          40     40     40
     5  PM Cooling Device 5             On          40     40     40
     6  PM Cooling Device 6             On          40     40     40
Management Modules
     1  CMM 1 (NP)                                   0     20     20
     2  SN#Y031BG18Y03L                  On         20     20     20
I/O Modules
     1  Ethernet ScSE                    On         29     64     64
     2  I/O Module 2 (NP)                           0    175    175
     3  Fibre ScSE                      On          39     45     45
     4  Fibre ScSE                      On          38     50     50
Blades
   1-4  Enclosure 01
     1    Discovering                   Off       104    730    730
Getting power allocation for blade[2] failed
Getting duty cycle numbers of blade[2] failed.
     2    Discovering                   Off         0      0      0
   5-8  Enclosure 05
     1    Discovering (C)              Off          0    638    638
     2    Discovering (C)              Off          0      0      0
     9  Node 09                          Off         6    107     72
    13  Discovering                     Off         0      0      0

Domain totals:
  Allocated Power                                 614   2849   2814

Note: (T) means "throttled", (U) means "unable to power up",
      * means "the blade may throttle", (NP) means "the module is not present",
      (D) means "discovering", (C) means "comm error", (SB) means "Standby"
      (CA) means "capped max power allocation"
-pm nonred

system> fuelg -pt 6
Date     Time     Avg Pwr
-------- -------- -------
10/29/12 19:45:00     784
10/29/12 19:50:00     792
10/29/12 19:55:00     784
10/29/12 20:00:00     787
10/29/12 20:05:00     787
10/29/12 20:10:00     784
10/29/12 20:15:00     784
10/29/12 20:20:00     782
10/29/12 20:25:01     786
system> fuelg -T blade[9]
PM Capability: Dynamic Power Measurement
Effective CPU Speed:    0 MHz
Maximum CPU Speed: 1900 MHz
Maximum Power:    6
```

```
Minimum Power:    6
Average Power:    6
Data captured at 10/29/12 20:25:03
system> fuelg -T mt[1] -tt 1
                          Temp  (C)
Date       Time       Max     Min     Avg
-------- -------- ------ ------ ------
02/06/14  12:20:01   25.50   24.50   24.90
02/06/14  12:24:59   25.50   24.50   24.80
02/06/14  12:30:01   27.00   25.50   26.20
system>
```

## groups command

This command displays and configures Active Directory groups of the primary CMM. This group information is used only when LDAP servers are enabled for authentication with local authorization.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "groups command errors" on page 437 for a list of error messages that are specific to the groups command.

*Table 43. groups (Active Directory groups) command*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display all Active Directory groups** | Displays all Active Directory groups, up to 16, configured for the Lenovo Flex System chassis. | `groups` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Display specific Active Directory group** | Displays information for the specified Active Directory group. | `groups -n` *group_name*<br>*group_name* is the unique alphanumeric string, up to 63 characters in length, that identifies the Active Directory group. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 43. groups (Active Directory groups) command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Add new Active Directory group** | Adds a new Active Directory group.<br>**Notes:** When adding a new group you must specify:<br>• a unique group name using the `-n` command option.<br>• a role-based security level for the group using the `-a` command option. | `groups -add -n` *group_name* `-a` *group_authority* where:<br>• *group_name* is a alphanumeric string up to 63 characters in length that can include periods ( . ) and underscores ( _ ). Each of the 16 group names must be unique.<br>• *group_authority* uses the following syntax:<br>– `operator` (Operator)<br>– `rbs:`*roles*`:`*scope* where the *roles* are one or more of the following authority levels, separated by a vertical bar ( \| ):<br>– `super` (Supervisor)<br>– `cam` (Chassis User Account Management)<br>– `clm` (Chassis Log Management)<br>– `co` (Chassis Operator)<br>– `cc` (Chassis Configuration)<br>– `ca` (Chassis Administration)<br>– `bo` (Blade Operator)<br>– `brp` (Blade Remote Present)<br>– `bc` (Blade Configuration)<br>– `ba` (Blade Administration)<br>– `so` (I/O Module Operator)<br>– `sc` (I/O Module Configuration)<br>– `sa` (I/O Module Administration)<br>*(continued on next page)* | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Add new Active Directory group** *(continued)* | | where the *scope* is one or more of the following devices, separated by a vertical bar ( \| ). Ranges of devices are separated by a dash ( - ). | |

*Table 43. groups (Active Directory groups) command (continued)*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | | • `c` *n* (Chassis *n*, where *n* is 1 for the Active Directory environment.)<br>• `b` *n* (Blade *n*, where *n* is a valid node bay number in the chassis)<br>• `s` *n* (I/O module *n*, where *n* is a valid I/O-bay number in the chassis)<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | |
| **Set Active Directory group authority level** | Sets the authority level for the specified Active Directory group. | `groups -n` *group_name* `-a` *group_authority*<br>where:<br>• *group_name* is the unique alphanumeric string, up to 63 characters in length, that identifies the Active Directory group.<br>• *group_authority* uses the following syntax:<br>– `operator` (Operator)<br>– `rbs:`*roles*`:`*scope* where the *roles* are one or more of the following authority levels, separated by a vertical bar ( \| ):<br>– `super` (Supervisor)<br>– `cam` (Chassis User Account Management)<br>– `clm` (Chassis Log Management)<br>– `co` (Chassis Operator)<br>– `cc` (Chassis Configuration)<br>– `ca` (Chassis Administration)<br>– `bo` (Blade Operator) | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 43. groups (Active Directory groups) command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | | – `brp` (Blade Remote Present)<br>– `bc` (Blade Configuration)<br>– `ba` (Blade Administration)<br>– `so` (I/O Module Operator)<br>– `sc` (I/O Module Configuration)<br>– `sa` (I/O Module Administration)<br>*(continued on next page)* | |
| **Set Active Directory group authority level** *(continued)* | | where the *scope* is one or more of the following devices, separated by a vertical bar ( \| ). Ranges of devices are separated by a dash ( - ).<br>• `c` *n* (Chassis *n*, where *n* is 1 for the Active Directory environment.)<br>• `b` *n* (Blade *n*, where *n* is a valid node bay number in the chassis)<br>• `s` *n* (I/O module *n*, where *n* is a valid I/O-bay number in the chassis)<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | |

Table 43. groups (Active Directory groups) command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Delete Active Directory group** | Delete the specified Active Directory group. | `groups -n` *group_name* `-clear`<br>*group_name* is the unique alphanumeric string, up to 63 characters in length, that identifies the Active Directory group.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

**Example:** To create an Active Directory group with a group name of admin1 that has supervisor rights to all Lenovo Flex System components, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
groups -add -n admin1 -a rbs:super -T mm[p]
```

To display information for the group named admin1, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
groups -n admin1 -T mm[p]
```

To change the security role of the group named admin1 to blade administration with a scope of compute nodes 1 through 14 (all compute nodes), while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
groups -n admin1 -a rbs:ba:b1-b14 -T mm[p]
```

To delete the group named admin1, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
groups -n admin1 -clear -T mm[p]
```

The following example shows the information that is returned from these commands:

```
system> groups -add -n admin1 -a rbs:super -T mm[p]
OK
system> groups -n admin1  -T mm[p]

-a Role:supervisor
   Blades:1|2|3|4|5|6|7|8|9|10|11|12|13|14
   Chassis:1
   Modules:1|2|3|4

system> groups -n admin1 -a rbs:ba:b1-b14 -T mm[p]
OK
system> groups -n admin1 -clear -T mm[p]
OK
system>
```

## health command

This command displays the current health status of the command target. It can also be used to display the alerts that are active for the command target.

You can only specify one command target each time you run the health command.

Results returned by the health command vary based on the command target and Flex System chassis type where the command target is installed.

- **Flex System Enterpise chassis command target:** For the Flex System Enterpise chassis command target, one of the following health states is returned. This state will reflect the highest health state reported by any other component installed in the chassis, unless the state reported by the chassis itself is higher.
  - OK - All monitored parameters are within normal their operating ranges.
  - System level - There are currently active minor warnings or system events, but no critical or major events are active.
  - Non-critical - There are currently active major warnings or system events, but no critical events are active.
  - Critical - One or more critical events are currently active.
- **Lenovo Flex System Carrier-Grade chassis command target:** For the Lenovo Flex System Carrier-Grade chassis command target, one of the following health states is returned. This state will reflect the highest health state reported by any other component installed in the chassis, unless the state reported by the chassis itself is higher.
  - OK - All monitored parameters are within normal their operating ranges.
  - Minor - There are currently active minor warnings or system events, but no critical or major events are active.
  - Major - There are currently active major warnings or system events, but no critical events are active.
  - Critical - One or more critical events are currently active.
- **Compute node command target:** For the compute node command target, one of the following health states is returned for all chassis types. This state will reflect the highest health state reported by any other component installed in the compute node, unless the state reported by the compute node itself is higher.
  - OK - All monitored parameters in the chassis are within normal their operating ranges.
  - Non-critical - There are currently active warnings or system events, but no critical events are active.
  - Critical - One or more critical events are currently active.
- **Command targets other than a chassis or compute node:** For command targets other than a compute node, one of the following health states is returned for all chassis types.
  - OK - All monitored parameters are within normal their operating ranges.
  - System level - There are currently active minor warnings or system events, but no critical or major events are active.
  - Non-critical - There are currently active major warnings or system events, but no critical events are active.
  - Critical - One or more critical events are currently active.

**Notes:** The various CMM interfaces use different terms to indicate the same condition:

- Web interface: Critical ⊗, Attention ⚠ (Telco major/minor event), Normal ✅ (Telco OK event)
- SNMP: Critical/Bad, Warning (Telco major/minor event), Good (Telco OK event)

- CLI: Critical, Non-critical (Telco major/minor event), OK

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See “Common errors” on page 407 for a list of error messages that apply to all commands or “health command errors” on page 438 for a list of error messages that are specific to the health command.

*Table 44. health command*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display health status** | Displays the current health status of the command target.<br>• Possible return values for the Flex System Enterpise chassis target are:<br>– ok<br>– system level<br>– non-critical<br>– critical<br>• Possible return values for the Lenovo Flex System Carrier-Grade chassis target are:<br>– ok<br>– minor<br>– major<br>– critical<br>• Possible return values for the compute node target are:<br>– ok<br>– non-critical<br>– critical<br>• Possible return values for other targets are:<br>– ok<br>– system level<br>– non-critical<br>– critical | `health` | Lenovo Flex System chassis:<br>`system`<br>Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number.<br>Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number.<br>I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number.<br>Power supply:<br>`power[`*x*`]`<br>where *x* is the power supply bay number.<br>Fan module:<br>`blower[`*x*`]`<br>where *x* is the fan module bay number. |
| **Display health status for tree** | Displays the current health status of the tree structure of devices present in the Lenovo Flex System chassis, starting at the command target level. If CMM bays are part of the tree, they will be identified as primary or standby (redundant).<br>• Possible return values for the Flex System Enterpise chassis target are:<br>– ok<br>– system level<br>– non-critical<br>– critical<br>• Possible return values for the Lenovo Flex System Carrier-Grade chassis target are:<br>– ok<br>– minor | `health -l` *depth*<br>where *depth*<br>• 1 displays health status of the current command target<br>• `2` , `all` , or `a` displays a full tree display, starting at the command target level | Lenovo Flex System chassis:<br>`system`<br>Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number.<br>Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |

Table 44. health command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | – major<br>– critical<br>• Possible return values for the compute node target are:<br>– ok<br>– non-critical<br>– critical<br>• Possible return values for other targets are:<br>– ok<br>– system level<br>– non-critical<br>– critical | | I/O module:<br>`switch[`*x*`]` where *x* is the I/O-bay number.<br>Power supply:<br>`power[`*x*`]` where *x* is the power supply bay number.<br>Fan module:<br>`blower[`*x*`]` where *x* is the fan module bay number. |
| **Display health status and alerts**<br>**Note:** This command option applies only to CMMs installed in a Lenovo Flex System Enterprise chassis. | Displays the current health status and active alerts for the command target.<br>• Possible return values for the Flex System Enterprise chassis target are:<br>– ok<br>– system level<br>– non-critical<br>– critical<br>• Possible return values for the compute node target are:<br>– ok<br>– non-critical<br>– critical<br>• Possible return values for other targets are:<br>– ok<br>– system level<br>– non-critical<br>– critical<br>• Active alert information provides short text descriptions of alerts that are active for each monitored component.<br>The total amount of information returned from the `health -f` command is limited to 1024 bytes. | `health -f` | Lenovo Flex System chassis:<br>`system`<br>Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]` where *x* is the primary CMM bay number.<br>Compute node:<br>`blade[`*x*`]` where *x* is the node bay number.<br>I/O module:<br>`switch[`*x*`]` where *x* is the I/O-bay number.<br>Power supply:<br>`power[`*x*`]` where *x* is the power supply bay number.<br>Fan module:<br>`blower[`*x*`]` where *x* is the fan module bay number. |

*Table 44. health command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display health status and active events (Telco)**<br>**Note:** This command option applies only to CMMs installed in a Lenovo Flex System Carrier-Grade chassis. | Displays the current health status and active events for the command target.<br>**Note:** In a Lenovo Flex System Carrier-Grade chassis, the -f option must be used exclusive of the -k option.<br>• Possible return values for the Lenovo Flex System Carrier-Grade chassis target are:<br>– ok<br>– minor<br>– major<br>– critical<br>• Possible return values for the compute node target are:<br>– ok<br>– non-critical<br>– critical<br>• Possible return values for other targets are:<br>– ok<br>– system level<br>– non-critical<br>– critical<br>• Active alert information provides short text descriptions of alerts that are active for each monitored component.<br>The total amount of information returned from the `health -f` command is limited to 1024 bytes. | `health -f` | Lenovo Flex System chassis:<br>`system`<br>Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number.<br>Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number.<br>I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number.<br>Power supply:<br>`power[`*x*`]`<br>where *x* is the power supply bay number.<br>Fan module:<br>`blower[`*x*`]`<br>where *x* is the fan module bay number. |
| **Display health status and acknowledged events (Telco)**<br>**Note:** This command option applies only to CMMs installed in a Lenovo Flex System Carrier-Grade chassis. | Displays the current health status and acknowledged events for the command target.<br>**Note:** In a Lenovo Flex System Carrier-Grade chassis, the -k option must be used exclusive of the -f option.<br>• Possible return values for the Lenovo Flex System Carrier-Grade chassis target are:<br>– ok<br>– minor<br>– major<br>– critical<br>• Possible return values for the compute node target are:<br>– ok<br>– non-critical<br>– critical | `health -k` | Lenovo Flex System chassis:<br>`system`<br>Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number.<br>Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |

Table 44. health command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | • Possible return values for other targets are:<br>– ok<br>– system level<br>– non-critical<br>– critical<br>• Active alert information provides short text descriptions of alerts that are active for each monitored component.<br>The total amount of information returned from the `health -f` command is limited to 1024 bytes. | | I/O module:<br>`switch[`*x*`]` where *x* is the I/O-bay number.<br>Power supply:<br>`power[`*x*`]` where *x* is the power supply bay number.<br>Fan module:<br>`blower[`*x*`]` where *x* is the fan module bay number. |
| **Display results with timestamp** | Adds display of timestamp information to status command output. | `health -t`<br>**Note:** The -t option must be used with the -f option. | Lenovo Flex System chassis:<br>`system`<br>Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]` where *x* is the primary CMM bay number.<br>Compute node:<br>`blade[`*x*`]` where *x* is the node bay number.<br>I/O module:<br>`switch[`*x*`]` where *x* is the I/O-bay number.<br>Power supply:<br>`power[`*x*`]` where *x* is the power supply bay number.<br>Fan module:<br>`blower[`*x*`]` where *x* is the fan module bay number. |

**Example:** To display the health status and alerts in a tree structure with time stamps for all components installed in the Lenovo Flex System Carrier-Grade Chassis, that are valid command targets, while the chassis is set as the default command target, at the `system>` prompt, type

```
health -l a -f -t
```

The following example shows the information that is returned from these commands:

```
system> health -l a -f -t
system   :                     Critical
         blade[1]  :          Critical
         (03/25/15, 16:29:58) (0000BB5C) Node Node 01 message: processor 2 has a Configuration Mismatch.
         blade[3]  :          Critical
         (03/25/15, 16:29:45) (0000BB58) Node Node 03 message: Front panel board 1, interconnect
(LightPath) configuration error.
         (03/25/15, 16:29:45) (0000BB59) Node Node 03 message: Expansion card 1, (Mezz Exp 1 Fault)
critical.
         (03/25/15, 16:30:11) (0000BB62) Node Node 03 incompatible with the I/O-module configuration.
         (03/25/15, 16:29:13) (0000BB47) Security policy is in Pending state at system-management
processor on Node 03.
         blade[5]  :          Non-Critical
         (03/25/15, 16:29:08) (0000BB46) Security policy is in Pending state at system-management
processor on Node 05.
         blade[6]  :          Non-Critical
         (03/25/15, 16:29:18) (0000BB4C) Security policy is in Pending state at system-management
processor on Node 06.
         blade[7]  :          Non-Critical
         (03/25/15, 16:29:30) (0000BB50) Node Node 07 device Storage back plane[01] VPD is not valid.
         (03/25/15, 16:29:35) (0000BB52) Node Node 07 device Storage back plane[02] VPD is not valid.
         blade[11] :          Critical
         (03/25/15, 16:48:33) (0000BB6F) Node Node 11 failed initial provisioning.
         blade[13] :          Non-Critical
         (03/25/15, 16:28:55) (0000BB43) Security policy is in Pending state at system-management
processor on Node 13.
         blade[14] :          Non-Critical
         (03/25/15, 16:28:51) (0000BB42) Security policy is in Pending state at system-management
processor on Node 14.
         (03/25/15, 16:29:05) (0000BB45) Node Node 14 device Expansion card[01] VPD is not valid.
         blower[1] :          OK
         blower[2] :          OK
         blower[3] :          Critical
         (03/25/15, 16:28:48) (0000BB40) Fan module Fan 03 has failed.
         blower[4] :          OK
         blower[5] :          OK
         blower[6] :          OK
         blower[7] :          OK
         blower[8] :          Critical
         (03/25/15, 16:29:01) (0000BB44) Fan module Fan 08 has failed.
         blower[9] :          OK
         blower[10]:          OK
         power[1]  :          Non-Critical
         (03/25/15, 16:29:15) (0000BB48) Power supply Power Supply 01 is off. Input fault.
                  blower[1] : OK
         power[2]  :          Non-Critical
         (03/25/15, 16:29:15) (0000BB49) Power supply Power Supply 02 is off. Input fault.
                  blower[1] : OK
         power[3]  :          Non-Critical
         (03/25/15, 16:29:15) (0000BB4A) Power supply Power Supply 03 is off. Input fault.
                  blower[1] : OK
         power[4]  :          OK
                  blower[1] : OK
```

```
          power[5]  :           OK
                    blower[1] : OK
          power[6]  :           Non-Critical
          (03/25/15, 16:29:16) (0000BB4B) Power supply Power Supply 06 is off. Input fault.
                    blower[1] : OK
          mm[1]      :           Non-Critical
          (03/25/15, 16:28:48) (0000BB41) Cooling zone zone01 might not have adequate cooling.
          mm[2]      :           OK
          switch[3] :           Non-Critical
          (03/25/15, 16:30:11) (0000BB61) I/O module IO Module 03 is incompatible with the node
configuration.
          mt[1]      :           OK
          fanmux[1] :           Non-Critical
          (03/25/15, 16:29:19) (0000BB4D) Fan logic module Fan Logic 01 is an older revision card (FRU
81Y2912) and needs to be replaced.
          fanmux[2] :           Non-Critical
          (03/25/15, 16:29:19) (0000BB4E) Fan logic module Fan Logic 02 is an older revision card (FRU
81Y2912) and needs to be replaced.
system>
```

## help command

This command displays a list of all commands that are available in the command-line interface with a brief description of each command.

You can also issue the help command by typing `?`. Adding a `-h`, `-help`, or `?` option to a command displays syntax help for the command.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "help command errors" on page 439 for a list of error messages that are specific to the help command.

*Table 45. help command*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Help** | Displays a list of commands and a brief description of each command. | `help` | Any installed device. |
| | | ? | Any installed device. |
| **Command help** | Displays help information for the specified command. | *command* `-h`<br>where *command* is any valid CLI root command (no options specified). | Any installed device. |
| | | *command* `-help`<br>where *command* is any valid CLI root command (no options specified). | Any installed device. |
| | | *command* ?<br>where *command* is any valid CLI root command (no options specified). | Any installed device. |

**Example:** To display a list of commands, while the CMM in bay 1 of a Flex System Carrier-Grade Chassis is set as the default command target, at the `system:mm[1]>` prompt, type

```
help
```

To obtain help about the `env` command, while the CMM in bay 1 of a Flex System Carrier-Grade Chassis is set as the default command target, at the `system:mm[1]>` prompt, type one of the following commands:

- `env -h`
- `env -help`
- `env ?`

The following example shows the information that is returned from these commands:

```
system:mm[1]> help
            ? -- Display commands
    accseccfg -- View/edit account security config
  advfailover -- View/edit advanced failover mode
    airfilter -- Manage the chassis air filter
        alarm -- Manage Telco System Management alarm(s)
     alertcfg -- Displays/configures the global remote alert settings
 alertentries -- View/edit remote alert recipients
      autoftp -- View/Edit auto ftp/tftp/sftp setting
      baydata -- View/edit Blade Bay Data string
     bootmode -- View/edit Boot mode
      bootseq -- View/edit the blade boot sequence settings
     chconfig -- View/edit Service Advisor Settings
        chlog -- Display Service Advisor Activity Log entires
     chmanual -- Manually generate call home request
       cimsub -- View/clear CIM subscriptions
          cin -- Displays/Configures Chassis Internal Network
    cinstatus -- Displays Status of Chassis Internal Network
        clear -- Clear the config
     clearlog -- Clear the event log
       config -- View/edit general settings
      console -- Start SOL session to a blade
 coolingzones -- View cooling zone information
       crypto -- View/edit cryptographic settings
         date -- View/edit date, time and time zone setting
     dhcpinfo -- View DHCP server assigned settings
   displaylog -- Display log entries
    displaysd -- Display service data
          dns -- View/edit DNS config
          env -- Set persistent command target
   ethoverusb -- View/edit the status of a blade SP's interface on Ethernet-over-USB
       events -- View/edit Events config
         exit -- Log off
        files -- Displays and deletes files stored on the CMM
          fod -- Display FoD licenses for management modules and switches
    fruactlog -- Displays FRU activity log
        fsmcm -- Disables FSM Central Management
        fuelg -- Power management
       groups -- View/edit Active Directory groups
       health -- View system health status
         help -- Display command list
      history -- Display command history
     ifconfig -- View/edit network interface config
         info -- Display identity and config of target
       iocomp -- View I/O compatibility for blades and switches
      ldapcfg -- View/edit LDAP config
          led -- Display and control Leds
         list -- Display installed targets
    monalerts -- Displays and configures monitored alerts
          ntp -- View/edit NTP config
   permgroups -- View/edit user permission group settings
         ping -- Pings targeted switches or blades
     pmpolicy -- View/edit power management policy settings
      portcfg -- Serial port configuration
        ports -- Port configuration
        power -- Control target power
   pwrprofile -- Display and configure the power schedules for groups of servers
         read -- Restore from a file containing CLI commands
remotechassis -- Chassis discovered over the network
        reset -- Reset target
        scale -- Display scalable complexes
       sddump -- Initiate service data dump
      sdemail -- Send service information using e-mail
     security -- View/edit security config
      service -- Displays aux power status and performs service resets
         smtp -- View/edit SMTP config
         snmp -- View/edit SNMP config
          sol -- View SOL status and view/edit SOL config
       sshcfg -- View/edit SSH config
       sslcfg -- View/edit SSL config
       syslog -- View/edit syslog config
   tcpcmdmode -- View/edit TCP command mode config
        temps -- View temperatures
     trespass -- View/edit trespassing warning config
        uicfg -- View/edit user interface configuration
       update -- Update firmware from remote location
       uplink -- View/edit failover on network uplink loss config
        users -- View/edit user profiles
         vlan -- View/edit vlan config
        volts -- View voltages
        write -- Write a file containing CLI commands

Type "<command> -h" for individual command syntax help.
        [ ] is used for indexing (by bay number)
        < > denotes a variable
        { } denotes optional arguments
         |  denotes choice
system:mm[1]> env ?
env -T <target>
where <target> is a full or relative target path. Example full target paths are:
 system
 system:mm[x]
 system:blade[x]
 system:blade[x]:sp
 system:switch[x]
 system:power[x]
 system:blower[x]
 system:mt[x]
 system:fanmux[x]
Note: To see a list of all installed targets, please use the 'list' command.
system:mm[1]>
```

## history command

This command displays the last eight commands that were entered, allowing the user to choose and re-enter one of these commands.

You choose the command to re-enter from the displayed list by typing an exclamation point (!) followed immediately by the numeric designation the command is assigned in the list. You can also recall one of the past eight previously entered commands using the up-arrow and down-arrow keys.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See “Common errors” on page 407 for a list of error messages that apply to all commands or “history command errors” on page 439 for a list of error messages that are specific to the history command.

*Table 46. history command*

| **Function** | **What it does** | **Command** | **Target** *(see paths in “Command targets” on page 6)* |
|---|---|---|---|
| **Command history** | Displays the last eight commands that were entered. | `history` | Any installed device. |
| **Re-enter previous command using numeric designation** | Re-enters a numerically-specified command from the command history. | ! *x*<br>where *x* is the number of the command (0 - 7) to re-enter from the command history list. | Any installed device. |

**Example:** To display a list of the last eight commands entered, while the primary CMM in bay 1 is set as the default command environment, at the `system:mm[1]>` prompt, type

```
history
```

To re-enter the command designated by "2" in the command history, type

```
!2
```

The following example shows the information that is returned from these two commands:

```
system:mm[1]> history
 0 dns
 1 dns -on
 2 dns
 3 dns -i1 192.168.70.29
 4 dns
 5 dns -i1 192.168.70.29 -on
 6 dns
 7 history
system:mm[1]> !2
Enabled
-i1 192.168.70.29
-i2 0.0.0.0
-i3 0.0.0.0
system:mm[1]>
```

## ifconfig command

This command configures and displays the network interface settings for the CMM Ethernet interface, I/O-module Ethernet interface, and the compute node system-management processors and installed options.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See “Common errors” on page 407 for a list of error messages that apply to all commands or “ifconfig command errors” on page 439 for a list of error messages that are specific to the ifconfig command.

*Table 47. ifconfig command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display primary CMM Ethernet channel 0 configuration** | Displays the current configuration of Ethernet channel 0 for the primary CMM. Possible return values are:<br>• enabled<br>• disabled<br>• -i *static_ip_address* (dotted decimal IPv4 IP address format)<br>• -g *gateway_address* (dotted decimal IPv4 IP address format)<br>• -s *subnet_mask* (dotted decimal IPv4 IP address format)<br>• -n *hostname*<br>• -c *config_method*<br>• -r *data_rate*<br>• -d *duplex_mode*<br>• -m *mtu*<br>• -l *locally_administered_mac_addr*<br>• -b *burnedin_mac_address*<br>• -dn *domain_name*<br>• -ipv6 *ipv6_state*<br>• -ipv6static *static_ipv6_state*<br>• -i6 *static_ip_address* (IPv6 format)<br>• -p6 *address_prefix_length*<br>• -g6 *gateway-default_route*<br>• -dhcp6 *dhcpv6_state*<br>• -sa6 *ipv6_stateless_autoconfig_state*<br>If IPv6 is enabled, the link-local address *link_local_address* (for IPv6 connection) also displays.<br><br>If IPv6 and stateless auto-configuration (-sa6) are both enabled, the Stateless auto-config IP Addresses / Prefix Length *address_table* (table listing auto-generated IPv6 addresses and their prefix lengths) also displays.<br><br>If there are two CMMs installed in the chassis and the `advfailover` command is set to `noswap`, the following items also display:<br>• -f *floating_ip_address* (dotted decimal IPv4 IP address format)<br>• -f6 *floating_ip_address* (IPv6 format) | `ifconfig -eth0` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Display standby CMM Ethernet channel 0 configuration** | Displays the current configuration of Ethernet channel 0 for the standby CMM.<br>**Note:** If there are two CMMs installed in the chassis and the currently active `advfailover` setting | `ifconfig -eth0 -o` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]` |

Table 47. ifconfig command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | is `off`, there will be no current configuration of eth0 for the standby CMM.<br>Possible return values are:<br>• enabled<br>• disabled<br>• -i *static_ip_address* (dotted decimal IPv4 IP address format)<br>• -g *gateway_address* (dotted decimal IPv4 IP address format)<br>• -s *subnet_mask* (dotted decimal IPv4 IP address format)<br>• -n *hostname*<br>• -c *config_method*<br>• -r *data_rate*<br>• -d *duplex_mode*<br>• -m *mtu*<br>• -l *locally_administered_mac_addr*<br>• -b *burnedin_mac_address*<br>• -dn *domain_name*<br>• -ipv6 *ipv6_state*<br>• -ipv6static *static_ipv6_state*<br>• -i6 *static_ip_address* (IPv6 format)<br>• -p6 *address_prefix_length*<br>• -g6 *gateway-default_route*<br>• -dhcp6 *dhcpv6_state*<br>• -sa6 *ipv6_stateless_autoconfig_state*<br>If IPv6 is enabled, the link-local address *link_local_address* (for IPv6 connection) also displays.<br>If IPv6 and stateless auto-configuration (-sa6) are both enabled, the Stateless auto-config IP Addresses / Prefix Length *address_table* (table listing auto-generated IPv6 addresses and their prefix lengths) also displays. | | where *x* is the primary CMM bay number.<br>**Note:** Even though this command displays information for the standby CMM, it still must specify the primary CMM as the command target. |
| **Set primary CMM Ethernet channel 0 static IP address (IPv4)** | Sets the IPv4 static IP address for Ethernet channel 0 for the primary CMM.<br>**Notes:**<br>• Static IPv4 parameters can not be set when the IPv4 configuration method is set to DHCP.<br>• Changes made to the IPv4 configuration of the primary CMM take effect after the next reset of the primary CMM. | `ifconfig -eth0 -i` *ip_address*<br>where *ip_address* is the static IP address for Ethernet channel 0 in dotted decimal IP address format.<br>This command can only be run by users who have one or more of the following command authorities: | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 47. ifconfig command (continued)*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | • Including the `-apply` option when setting an IPv4 configuration option makes the change take effect immediately.<br>• Use the `-apply` option by itself after setting multiple IPv4 configuration options for an Ethernet channel to make all changes for that Ethernet channel take effect without resetting the primary CMM. | • Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | |
| **Apply IPv4 configuration for primary CMM** | Places all outstanding IPv4 configuration made to the primary CMM into effect.<br>**Note:** Using the -apply option places changes into effect without resetting the CMM. | `ifconfig -eth0 -apply`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set primary CMM Ethernet channel 0 static IP address (IPv6)** | Sets the IPv6 static IP address for Ethernet channel 0 for the primary CMM. | `ifconfig -eth0 -i6` *ip_address*<br>where *ip_address* is the static IP address for Ethernet channel 0 in IPv6 format.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 47. ifconfig command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set primary CMM Ethernet channel 0 floating IP address (IPv4)** | Sets the IPv4 floating IP address for Ethernet channel 0 for the primary CMM.<br>**Notes:**<br>• An Ethernet channel 0 floating IP address for the CMM can only be set if there are two CMMs installed in the chassis and the `advfailover` command is set to `noswap`.<br>• Changes made to the IPv4 configuration of the primary CMM take effect after the next reset of the primary CMM.<br>• Including the `-apply` option when setting an IPv4 configuration option makes the change take effect immediately.<br>• Use the `-apply` option by itself after setting multiple IPv4 configuration options for an Ethernet channel to make all changes for that Ethernet channel take effect without resetting the primary CMM. | `ifconfig -eth0 -f` *ip_address*<br>where *ip_address* is the floating IP address for Ethernet channel 0 in dotted decimal IP address format.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set primary CMM Ethernet channel 0 floating IP address (IPv6)** | Sets the IPv6 floating IP address for Ethernet channel 0 for the primary CMM.<br>**Note:** An Ethernet channel 0 floating IP address for the CMM can only be set if there are two CMMs installed in the chassis and the `advfailover` command is set to `noswap`. | `ifconfig -eth0 -f6` *ip_address*<br>where *ip_address* is the floating IP address for Ethernet channel 0 in IPv6 format.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 47. ifconfig command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set standby CMM Ethernet channel 0 static IP address (IPv4)** | Sets the IPv4 static IP address for Ethernet channel 0 for the standby CMM.<br>**Notes:**<br>• An Ethernet channel 0 floating IP address for the CMM can only be set if there are two CMMs installed in the chassis and the `advfailover` command is set to `noswap`.<br>• Static IPv4 parameters can not be set when the IPv4 configuration method is set to DHCP.<br>• Changing the IPv4 static IP address for the standby CMM takes effect immediately. | `ifconfig -eth0 -o -i` *ip_address*<br>where *ip_address* is the static IP address for Ethernet channel 0 in dotted decimal IP address format.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number.<br>**Note:** Even though this command displays information for the standby CMM, it still must specify the primary CMM as the command target. |
| **Set standby CMM Ethernet channel 0 static IP address (IPv6)** | Sets the IPv6 static IP address for Ethernet channel 0 for the standby CMM.<br>**Note:** An Ethernet channel 0 floating IP address for the CMM can only be set if there are two CMMs installed in the chassis and the `advfailover` command is set to `noswap`. | `ifconfig -eth0 -o -i6` *ip_address*<br>where *ip_address* is the static IP address for Ethernet channel 0 in IPv6 format.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number.<br>**Note:** Even though this command displays information for the standby CMM, it still must specify the primary CMM as the command target. |

*Table 47. ifconfig command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set primary CMM Ethernet channel 0 gateway IP address (IPv4)** | Sets the IPv4 gateway IP address for Ethernet channel 0 for the primary CMM.<br>**Notes:**<br>• Static IPv4 parameters can not be set when the IPv4 configuration method is set to DHCP.<br>• Changes made to the IPv4 configuration of the primary CMM take effect after the next reset of the primary CMM.<br>• Including the `-apply` option when setting an IPv4 configuration option makes the change take effect immediately.<br>• Use the `-apply` option by itself after setting multiple IPv4 configuration options for an Ethernet channel to make all changes for that Ethernet channel take effect without resetting the primary CMM. | `ifconfig -eth0 -g` *ip_address*<br>where *ip_address* is the gateway IP address for Ethernet channel 0 in dotted decimal IP address format.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set primary CMM Ethernet channel 0 gateway/default route (IPv6)** | Sets the IPv6 gateway/default route for Ethernet channel 0 for the primary CMM. | `ifconfig -eth0 -g6` *ip_address*<br>where *ip_address* is the gateway/default route for Ethernet channel 0 in IPv6 format.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 47. ifconfig command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set primary CMM Ethernet channel 0 subnet mask (IPv4)** | Sets the IPv4 subnet mask for Ethernet channel 0 for the primary CMM.<br>**Notes:**<br>• Static IPv4 parameters can not be set when the IPv4 configuration method is set to DHCP.<br>• Changes made to the IPv4 configuration of the primary CMM take effect after the next reset of the primary CMM.<br>• Including the `-apply` option when setting an IPv4 configuration option makes the change take effect immediately.<br>• Use the `-apply` option by itself after setting multiple IPv4 configuration options for an Ethernet channel to make all changes for that Ethernet channel take effect without resetting the primary CMM. | `ifconfig -eth0 -s` *sub_mask*<br>where *sub_mask* is the subnet mask for Ethernet channel 0 in dotted decimal IP address format.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set primaryCMM Ethernet channel 0 hostname** | Sets the host name for Ethernet channel 0 for the primary CMM.<br>**Notes:**<br>• Changes made to the IPv4 configuration of the primary CMM take effect after the next reset of the primary CMM.<br>• Including the `-apply` option when setting an IPv4 configuration option makes the change take effect immediately.<br>• Use the `-apply` option by itself after setting multiple IPv4 configuration options for an Ethernet channel to make all changes for that Ethernet channel take effect without resetting the primary CMM. | `ifconfig -eth0 -n` *hostname*<br>where *hostname* is the host name for Ethernet channel 0. The hostname can be a string up to 63 characters in length that includes alphanumeric characters, hyphens, and underscores.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 47. ifconfig command (continued)

| Function | What it does | Command | Target (see paths in "Command targets" on page 6) |
|---|---|---|---|
| **Set standby CMM Ethernet channel 0 hostname** | Sets the host name for Ethernet channel 0 for the standby CMM.<br>**Note:** Changes made to the host name of the standby CMM take effect immediately. | `ifconfig -eth0 -o -n` *hostname*<br>where *hostname* is the host name for Ethernet channel 0. The hostname can be a string up to 63 characters in length that includes alphanumeric characters, hyphens, and underscores.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number.<br>**Note:** Even though this command displays information for the standby CMM, it still must specify the primary CMM as the command target. |
| **Set primary CMM Ethernet channel 0 IPv4 configuration method** | Sets the IPv4 configuration method for Ethernet channel 0 for the primary CMM.<br>A value of `dthens` will try the DHCP configuration and default to the static IP configuration if DHCP is unsuccessful after 2 minutes.<br>**Notes:**<br>• If the CMM DHCP setting is set to try the DHCP server and then use the static IP address, the CMM will use the static IP address when the DHCP server is not available during CMM start up. When this occurs, the IP address might not be reachable if multiple CMMs were started with the same static IP address.<br>• Static IPv4 parameters can not be set when the IPv4 configuration method is set to DHCP.<br>• Changes made to the IPv4 configuration of the primary CMM take effect after the next reset of the primary CMM.<br>• Including the `-apply` option when setting an IPv4 configuration option makes the change take effect immediately.<br>• Use the `-apply` option by itself after setting multiple IPv4 configuration options for an Ethernet channel to make all | `ifconfig -eth0 -c` *config_method*<br>where *config_method* is<br>• `dhcp`<br>• `static`<br>• `dthens`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 47. ifconfig command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | changes for that Ethernet channel take effect without resetting the primary CMM. | | |
| **Set primary CMM Ethernet channel 0 data rate** | Sets the data rate for Ethernet channel 0 for the primary CMM.<br>**Note:** Changes made to the data rate of the primary CMM take effect after the next reset of the primary CMM. | `ifconfig -eth0 -r` *data_rate*<br>where *data_rate* is<br>- `10`<br>- `100`<br>- `auto`<br>- `1000auto`<br>**Note:** When set to 1000auto, the duplex mode is automatically changed to full.<br>This command can only be run by users who have one or more of the following command authorities:<br>- Supervisor<br>- Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set primary CMM Ethernet channel 0 duplex mode** | Sets the duplex mode for Ethernet channel 0 for the primary CMM.<br>**Note:** Changes made to the duplex mode of the primary CMM take effect after the next reset of the primary CMM. | `ifconfig -eth0 -d` *duplex_mode*<br>where *duplex_mode* is<br>- `auto`<br>- `half`<br>- `full`<br>This command can only be run by users who have one or more of the following command authorities:<br>- Supervisor<br>- Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 47. ifconfig command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set CMM Ethernet channel 0 MTU** | Sets the MTU (maximum transmission unit) for Ethernet channel 0 for the CMM. | `ifconfig -eth0 -m` *mtu* where *mtu* is between 60 and 1500, inclusive.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set primary CMM Ethernet channel 0 static MAC address (locally administered)** | Sets the locally administered MAC address to the specified MAC address for Ethernet channel 0 for the primary CMM.<br>**Note:** Changes made to the IP configuration of the primary CMM take effect after the next reset of the primary CMM. | `ifconfig -eth0 -l` *address* where *address* is the locally administered MAC address for Ethernet channel 0. The MAC address is 6 bytes in length, hexadecimal, separated by colons. The MAC address can not be a multicast address (the first byte must be even).<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 47. ifconfig command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set standby CMM Ethernet channel 0 static MAC address (locally administered)** | Sets the locally administered MAC address to the specified MAC address for Ethernet channel 0 for the standby CMM.<br>**Note:** Changes made to the locally administered MAC address of the standby CMM take effect immediately. | `ifconfig -eth0 -o -l` *address*<br>where *address* is the locally administered MAC address for Ethernet channel 0. The MAC address is 6 bytes in length, hexadecimal, separated by colons. The MAC address can not be a multicast address (the first byte must be even).<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number.<br>**Note:** Even though this command displays information for the standby CMM, it still must specify the primary CMM as the command target. |
| **Set primary CMM Ethernet channel 0 domain name** | Sets the domain name for Ethernet channel 0 for the primary CMM.<br>**Note:** Changes made to the IP configuration of the primary CMM take effect after the next reset of the primary CMM. | `ifconfig -eth0 -dn` *domain*<br>where *domain* is an alphanumeric string up to 127 characters in length. The domain name must contain at least one dot (.).<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 47. ifconfig command (continued)*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set standby CMM Ethernet channel 0 domain name** | Sets the domain name for Ethernet channel 0 for the standby CMM. | `ifconfig -o -eth0 -dn` *domain*<br>where *domain* is an alphanumeric string up to 127 characters in length. The domain name must contain at least one dot (.).<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Enable / disable static IPv6 configuration for CMM Ethernet channel 0** | Enable or disable static IPv6 configuration for Ethernet channel 0 for the CMM. | `ifconfig -eth0 -ipv6static` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set CMM Ethernet channel 0 address prefix length** | Sets the IPv6 address prefix length for Ethernet channel 0 for the CMM. | `ifconfig -eth0 -p6` *length*<br>where *length* is between 1 and 128 (inclusive).<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 47. ifconfig command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Enable / disable DHCPv6 for CMM Ethernet channel 0** | Enable or disable static DHCPv6 for Ethernet channel 0 for the CMM. | `ifconfig -eth0 -dhcp6` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Enable / disable IPv6 stateless auto-configuration for CMM for Ethernet channel 0** | Enable or disable IPv6 stateless auto-configuration for Ethernet channel 0 for the CMM. | `ifconfig -eth0 -sa6` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Display network configuration status for compute node** | Displays the network interfaces and network status for the specified compute node. | `ifconfig` | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |
| **Display configuration information for network interface** | Displays the network interface type and number (such as -eth0), network interface state (up or down), and other network interface configuration information for the specified network interface in the specified compute node. | `ifconfig` -*interface_label*<br>where *interface_label* is any interface label reported by the compute node that specifies both the interface type and channel number. For example, `eth0` for Ethernet channel 0. Valid interface types include:<br>• `usb` for USB<br>• `eth` for Ethernet<br>Valid interface types for a specific compute node can be seen by running the `ifconfig` command with no interface argument. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |

Table 47. ifconfig command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set compute node network interface static IP address (IPv4)** | Sets the IPv4 static IP address for the specified network interface of the specified compute node.<br>**Notes:**<br>• This command will run only if the target compute node supports manual configuration of its management network interface.<br>• Static IPv4 parameters can not be set when the IPv4 configuration method is set to DHCP. | `ifconfig` -*interface_label* `-i` *ip_address*<br>where:<br>• *interface_label* is any interface label reported by the compute node that specifies both the interface type and channel number. For example, `eth0` for Ethernet channel 0. Valid interface types include:<br>– `usb` for USB<br>– `eth` for Ethernet<br>• *ip_address* is the static IP address for network interface in dotted decimal IP address format.<br>Valid interface types for a specific compute node can be seen by running the `ifconfig` command with no interface argument.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade configuration<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |
| **Set compute node network interface static IP address (IPv6)** | Sets the IPv6 static IP address for the specified network interface of the specified compute node.<br>**Notes:**<br>• This command will run only if the target compute node supports manual IPv6 configuration of its management network interface.<br>• A static IPv6 configuration ID is required for network interfaces that support more than one static configuation. | `ifconfig` -*interface_label* `-i6` *ip_address* `-id` *id*<br>where:<br>• *interface_label* is any interface label reported by the compute node that specifies both the interface type and channel number. For example, `eth0` for Ethernet channel 0. Valid interface types include:<br>– `usb` for USB<br>– `eth` for Ethernet<br>• *ip_address* is the static IP address for Ethernet | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |

Table 47. ifconfig command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | | channel *x* in IPv6 format.<br>• *id* is the static IPv6 configuration ID.<br><br>Valid interface types for a specific compute node can be seen by running the `ifconfig` command with no interface argument.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade configuration<br>See "Commands and user authority" on page 10 for additional information. | |
| **Set compute node network interface gateway IP address (IPv4)** | Sets the IPv4 gateway IP address for the specified network interface of the specified compute node.<br>**Notes:**<br>• This command will run only if the target compute node supports manual configuration of its management network interface.<br>• Static IPv4 parameters can not be set when the IPv4 configuration method is set to DHCP. | `ifconfig -`*interface_label* `-g` *ip_address*<br>where:<br>• *interface_label* is any interface label reported by the compute node that specifies both the interface type and channel number. For example, `eth0` for Ethernet channel 0. Valid interface types include:<br>– `usb` for USB<br>– `eth` for Ethernet<br>• *ip_address* is the gateway IP address for Ethernet channel *x* in dotted decimal IP address format.<br><br>Valid interface types for a specific compute node can be seen by running the `ifconfig` command with no interface argument.<br><br>This command can only be run by users who have one or more of the following command authorities: | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |

*Table 47. ifconfig command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | | • Supervisor<br>• Blade configuration<br>See "Commands and user authority" on page 10 for additional information. | |
| **Set compute node network interface gateway/default route (IPv6)** | Sets the IPv6 gateway/default route for the specified network interface of the specified compute node.<br>**Notes:**<br>• This command will run only if the target compute node supports manual IPv6 configuration of its management network interface..<br>• A static IPv6 configuration ID is required for network interfaces that support more than one static configuation. | `ifconfig` -*interface_label* `-g6` *ip_address* `-id` *id*<br>where:<br>• *interface_label* is any interface label reported by the compute node that specifies both the interface type and channel number. For example, `eth0` for Ethernet channel 0. Valid interface types include:<br>– `usb` for USB<br>– `eth` for Ethernet<br>• *ip_address* is the gateway/default route for Ethernet channel *x* in IPv6 format.<br>• *id* is the static IPv6 configuration ID.<br><br>Valid interface types for a specific compute node can be seen by running the `ifconfig` command with no interface argument.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade configuration<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |

*Table 47. ifconfig command (continued)*

| Function | What it does | Command | **Target** *(see paths in "*Command targets*" on page 6)* |
|---|---|---|---|
| **Set compute node network interface subnet mask (IPv4)** | Sets the IPv4 subnet mask for the specified network interface of the specified compute node.<br>**Notes:**<br>- This command will run only if the target compute node supports manual configuration of its management network interface.<br>- Static IPv4 parameters can not be set when the IPv4 configuration method is set to DHCP. | `ifconfig` -*interface_label* `-s` *sub_mask*<br>where:<br>- *interface_label* is any interface label reported by the compute node that specifies both the interface type and channel number. For example, `eth0` for Ethernet channel 0. Valid interface types include:<br>– `usb` for USB<br>– `eth` for Ethernet<br>- *sub_mask* is the subnet mask for Ethernet channel *x* in dotted decimal IP address format.<br><br>Valid interface types for a specific compute node can be seen by running the `ifconfig` command with no interface argument.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>- Supervisor<br>- Blade configuration<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |
| **Set compute node network interface IPv4 configuration method** | Sets the IPv4 configuration method for the specified network interface of the specified compute node.<br>A value of `dthens` will try the DHCP configuration and default to the static IP configuration if DHCP is unsuccessful after 2 minutes.<br>**Notes:**<br>- This command will run only if the target compute node supports manual configuration of its management network interface.<br>- If the DHCP setting is set to try the DHCP server and then use the static IP address, the NIC will use the static IP address when the DHCP server is not available | `ifconfig` -*interface_label* `-c` *config_method*<br>where:<br>- *interface_label* is any interface label reported by the compute node that specifies both the interface type and channel number. For example, `eth0` for Ethernet channel 0. Valid interface types include:<br>– `usb` for USB<br>– `eth` for Ethernet<br>- *config_method* is<br>– `dhcp` | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |

Table 47. ifconfig command (continued)

| Function | What it does | Command | Target (see paths in "Command targets" on page 6) |
|---|---|---|---|
| | during start up. When this occurs, the IP address might not be reachable if multiple devices were started with the same static IP address.<br>- If the CMM and compute nodes are set up to use DHCP and the CMM loses network connectivity, the CMM will attempt to acquire a new IP address when network connectivity is restored. The compute nodes will not attempt to acquire an IP address again; they will continue using their existing IP addresses. If you experience compute node network problems after connectivity between the CMM and network is restored, you might need to reset the system-management processor on each compute node in the chassis (including optional Lenovo XClarity Administrator or Flex System Manager hardware, if it is installed).<br>- Static IPv4 parameters can not be set when the IPv4 configuration method is set to DHCP. | – `static`<br>– `dthens`<br><br>Valid interface types for a specific compute node can be seen by running the `ifconfig` command with no interface argument.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>- Supervisor<br>- Blade configuration<br>See "Commands and user authority" on page 10 for additional information. | |
| **Enable / disable IPv4 addressing for compute node** | Enable or disable IPv4 addressing for the specified network interface of the specified compute node. | `ifconfig -`*interface_label* `-ipv4` *state*<br>where:<br>- *interface_label* is any interface label reported by the compute node that specifies both the interface type and channel number. For example, `eth0` for Ethernet channel 0. Valid interface types include:<br>– `usb` for USB<br>– `eth` for Ethernet<br>- *state* is `enabled` or `disabled`.<br><br>Valid interface types for a specific compute node can be seen by running the `ifconfig` command with no interface argument. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |

Table 47. ifconfig command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | | This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade configuration<br>See "Commands and user authority" on page 10 for additional information. | |
| **Set compute node address prefix length** | Sets the IPv6 address prefix length for the specified network interface of the specified compute node.<br>**Notes:**<br>• This command will run only if the target compute node supports manual IPv6 configuration of its management network interface.<br>• A static IPv6 configuration ID is required for network interfaces that support more than one static configuation. | `ifconfig` -*interface_label* `-p6` *length* `-id` *id*<br>where:<br>• *interface_label* is any interface label reported by the compute node that specifies both the interface type and channel number. For example, `eth0` for Ethernet channel 0. Valid interface types include:<br>– `usb` for USB<br>– `eth` for Ethernet<br>• *length* is between 1 and 128 (inclusive).<br>• *id* is the static IPv6 configuration ID.<br>Valid interface types for a specific compute node can be seen by running the `ifconfig` command with no interface argument.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade configuration<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |

*Table 47. ifconfig command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Enable / disable DHCPv6 for compute node** | Enable or disable static DHCPv6 for the specified network interface of the specified compute node.<br>**Note:** This command will run only if the target compute node supports manual IPv6 configuration of its management network interface. | `ifconfig` -*interface_label* `-dhcp6` *state*<br>where:<br>• *interface_label* is any interface label reported by the compute node that specifies both the interface type and channel number. For example, `eth0` for Ethernet channel 0. Valid interface types include:<br>– `usb` for USB<br>– `eth` for Ethernet<br>• *state* is `enabled` or `disabled` .<br>Valid interface types for a specific compute node can be seen by running the `ifconfig` command with no interface argument.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade configuration<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |
| **Enable / disable IPv6 stateless auto-configuration for compute node** | Enable or disable IPv6 stateless auto-configuration for the specified network interface of the specified compute node.<br>**Note:** This command will run only if the target compute node supports manual IPv6 configuration of its management network interface. | `ifconfig` -*interface_label* `-sa6` *state*<br>where:<br>• *interface_label* is any interface label reported by the compute node that specifies both the interface type and channel number. For example, `eth0` for Ethernet channel 0. Valid interface types include:<br>– `usb` for USB<br>– `eth` for Ethernet<br>• *state* is `enabled` or `disabled`<br>Valid interface types for a specific compute node | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |

Table 47. ifconfig command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | | can be seen by running the `ifconfig` command with no interface argument.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade configuration<br>See "Commands and user authority" on page 10 for additional information. | |
| **Display network settings for I/O module** | Displays network settings for the specified I/O module. Valid return values are:<br>• I/O-module type<br>• -i *ip_address* (dotted decimal IPv4 IP address format)<br>• -s *subnet_mask* (dotted decimal IPv4 IP address format)<br>• -g *gateway_address* (dotted decimal IPv4 IP address format)<br>• -em *ext_mgt_status*<br>• -ep *non_mgmt_data_port_status*<br>• -pm *enabled/disabled* (protected mode)<br>• -pip *enabled/disabled*<br>• -c *config_method*<br>• -ipv6 *ipv6_state*<br>• -ipv6static *static_ipv6_state*<br>• -i6 *static_ip_address* (IPv6 format)<br>• -p6 *address_prefix_length* (IPv6 format)<br>• -g6 *gateway-default_route* (IPv6 format)<br>• -dhcp6 *dhcpv6_state*<br>• -sa6 *ipv6_stateless_autoconfig_state*<br>If IPv6 is enabled, the link-local address *link_local_address* (for IPv6 connection) also displays.<br>If IPv6 and stateless auto-configuration (-sa6) are both enabled, the Stateless auto-config IP Addresses / Prefix Length *address_table* (table listing auto-generated IPv6 addresses and their prefix lengths) also displays. | `ifconfig` | I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |

*Table 47. ifconfig command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set I/O module IPv4 network configuration method** | Sets the IPv4 network configuration method for the specified I/O module.<br>A value of `dthens` will try the DHCP configuration and default to the static IP configuration if DHCP is unsuccessful after 2 minutes.<br>**Notes:**<br>• This command will run only if the target I/O module supports manual configuration of its management network interface.<br>• If the DHCP setting is set to try the DHCP server and then use the static IP address, the I/O module will use the static IP address when the DHCP server is not available during start up. When this occurs, the IP address might not be reachable if multiple devices were started with the same static IP address.<br>• Static IPv4 parameters can not be set when the IPv4 configuration method is set to DHCP. | `ifconfig -c` *config_method*<br>where *config_method* is<br>• `dhcp`<br>• `static`<br>• `dthens`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• I/O module configuration<br>See "Commands and user authority" on page 10 for additional information. | I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |
| **Set starting IP address for I/O module (IPv4)** | Sets the IPv4 IP addresses for the specified I/O module.<br>**Note:** Static IPv4 parameters can not be set when the IPv4 configuration method is set to DHCP. | `ifconfig -i` *ip_address*<br>where *ip_address* is the IP address of the specified I/O module in dotted decimal IP address format.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• I/O module configuration<br>See "Commands and user authority" on page 10 for additional information. | I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |

*Table 47. ifconfig command (continued)*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set starting IP address for I/O module (IPv6)** | Sets the IPv6 static IP address for the specified I/O module. | `ifconfig -i6` *ip_address* where *ip_address* is the static IP address for the specified I/O module in IPv6 format.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• I/O module configuration<br>See "Commands and user authority" on page 10 for additional information. | I/O module:<br>`switch[`*x*`]` where *x* is the I/O-bay number. |
| **Set I/O-module gateway IP address (IPv4)** | Sets the gateway IPv4 IP address for the specified I/O module.<br>**Note:** Static IPv4 parameters can not be set when the IPv4 configuration method is set to DHCP. | `ifconfig -g` *ip_address* where *ip_address* is the gateway IP address for the I/O module in dotted decimal IP address format.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• I/O module configuration<br>See "Commands and user authority" on page 10 for additional information. | I/O module:<br>`switch[`*x*`]` where *x* is the I/O-bay number. |
| **Set I/O-module gateway IP address (IPv6)** | Sets the IPv6 gateway/default route for the specified I/O module. | `ifconfig -g6` *ip_address* where *ip_address* is the gateway IP address for the I/O module in IPv6 format.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• I/O module configuration<br>See "Commands and user authority" on page 10 for additional information. | I/O module:<br>`switch[`*x*`]` where *x* is the I/O-bay number. |

*Table 47. ifconfig command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Keep new IP address configuration for I/O-module after reset** | Retains a new IP address configuration after the specified I/O module is reset.<br>**Note:** Make sure a valid New Static IP Configuration is entered for this I/O module so that when the module's manufacturing defaults are restored, or when a reset is initiated by a source other than the CMM, the New Static IP Configuration will be configured. In these cases CMM communication with the I/O module will be preserved. | `ifconfig -pip enabled`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• I/O module administration<br>• I/O module configuration<br>See "Commands and user authority" on page 10 for additional information. | I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |
| **Revert to old IP address configuration for I/O-module after reset** | Reverts IP address to old configuration after the specified I/O module is reset.<br>**Note:** The manufacturing default IP configuration will become active when the I/O module is reset to manufacturing defaults by either the CMM or the I/O module. If an I/O module reset is initiated by a source other than the CMM, then the previous IP configuration will be in affect. In both of these cases the CMM will lose IP communications with the I/O module. | `ifconfig -pip disabled`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• I/O module administration<br>• I/O module configuration<br>See "Commands and user authority" on page 10 for additional information. | I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |
| **Set I/O-module subnet mask (IPv4)** | Sets the IPv4 subnet mask for the specified I/O module.<br>**Note:** Static IPv4 parameters can not be set when the IPv4 configuration method is set to DHCP. | `ifconfig -s` *sub_mask*<br>where *sub_mask* is the subnet mask for the I/O module in dotted decimal IP address format.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• I/O module configuration<br>See "Commands and user authority" on page 10 for additional information. | I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |

*Table 47. ifconfig command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Enable / disable external management for I/O module** | Enables or disables external management on all ports for the specified I/O module. | `ifconfig -em` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• I/O module configuration<br>See "Commands and user authority" on page 10 for additional information. | I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |
| **Enable Ethernet interface for I/O module** | Enables the Ethernet interface for the specified I/O module. | `ifconfig -up`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• I/O module configuration<br>See "Commands and user authority" on page 10 for additional information. | I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |
| **Disable Ethernet interface for I/O module** | Disables the Ethernet interface for the specified I/O module. | `ifconfig -down`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• I/O module configuration<br>See "Commands and user authority" on page 10 for additional information. | I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |
| **Enable / disable non-management data ports for I/O module** | Enables or disables non-management data ports for the specified I/O module. | `ifconfig -ep` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• I/O module configuration<br>See "Commands and user authority" on page 10 for additional information. | I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |

*Table 47. ifconfig command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Enable / disable protected mode for I/O module** | Enables or disables protected mode for the specified I/O module. | `ifconfig -pm` *state*<br>where *state* is `enabled` or `disabled`.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• I/O module configuration<br>See "Commands and user authority" on page 10 for additional information. | I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |
| **Enable / disable static IPv6 configuration for I/O module** | Enable or disable static IPv6 configuration for the specified I/O module. | `ifconfig -ipv6static` *state*<br>where *state* is `enabled` or `disabled`.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• I/O module configuration<br>See "Commands and user authority" on page 10 for additional information. | I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |
| **Set I/O module address prefix length** | Sets the IPv6 address prefix length for the specified I/O module. | `ifconfig -p6` *length*<br>where *length* is between 1 and 128 (inclusive).<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• I/O module configuration<br>See "Commands and user authority" on page 10 for additional information. | I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |

Table 47. ifconfig command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Enable / disable DHCPv6 for I/O module** | Enable or disable static DHCPv6 for the specified I/O module. | `ifconfig -dhcp6` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• I/O module configuration<br>See "Commands and user authority" on page 10 for additional information. | I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |
| **Enable / disable IPv6 stateless auto-configuration for I/O module** | Enable or disable IPv6 stateless auto-configuration for the specified I/O module. | `ifconfig -sa6` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• I/O module configuration<br>See "Commands and user authority" on page 10 for additional information. | I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |

**Example:**

To set the CMM IPv4 static IP address for Ethernet channel 0 to 192.168.70.133, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type
`ifconfig -eth0 -i 192.168.70.133 -c static -T mm[p]`

The following example shows the information that is returned from this command:

```
system> ifconfig -eth0 -i 192.168.70.133 -c static -T mm[p]
Changes to -c, -i, -s, -g, and -f will become active after the next reset of the
CMM, or by using the -apply flag.
system>
```

To display the configuration for CMM Ethernet channel 0, after the above change has been applied, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type
`ifconfig -eth0 -T mm[p]`

The following example shows the information that is returned from this command:

```
system> ifconfig -eth0 -T mm[p]
Enabled
-i 192.168.70.133
```

```
-g 9.72.216.1
-s 255.255.248.0
-n MM5CF3FC25DC49
-c static
-r auto
-d auto
-m 1500
-l 00:00:00:00:00:00
-b 5C:F3:FC:25:DC:49
-dn cmm.com
-ipv6 enabled
-ipv6static disabled
-i6 ::
-p6 0
-g6 ::
-dhcp6 enabled
-sa6 enabled
Link-local address: fe80::5ef3:fcff:fe25:dc49
Stateless auto-config IP Addresses       Prefix Length
-----------------------------------------  -------------
3001:1013::5ef3:fcff:fe25:dc49           64
2000:1013::5ef3:fcff:fe25:dc49           64
3000:1013::5ef3:fcff:fe25:dc49           64
3002:1013::5ef3:fcff:fe25:dc49           64
2002:1013::5ef3:fcff:fe25:dc49           64
2001:1013::5ef3:fcff:fe25:dc49           64
system>
```

## info command

This command displays information about Lenovo Flex System components and their configuration.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See “Common errors” on page 407 for a list of error messages that apply to all commands or “info command errors” on page 444 for a list of error messages that are specific to the info command.

Table 48. info command

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display component information** | Displays identification and configuration information for the command target. | `info`<br>**Note:** Only one target at a time can be viewed with the info command. | Lenovo Flex System chassis:<br>`system`<br>Primary or standby CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[s]`<br>`mm[S]`<br>`mm[`*x*`]`<br>where *x* is the primary or standby CMM bay number.<br>Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number.<br>Fan logic module:<br>`fanmux[`*x*`]`<br>where *x* is the fan logic module bay number.<br>Fan module:<br>`blower[`*x*`]`<br>where *x* is the fan module bay number.<br>Compute node expansion adapter:<br>`exp[`*x*`]`<br>where *x* is the expansion adapter number.<br>Compute node management card:<br>`mgmtcrd[`*x*`]`<br>where *x* is the management card number.<br>Compute node system-management processor:<br>`sp`<br>*(continued on next page)* |

*Table 48. info command (continued)*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display component information** *(continued)* | | | Compute node expansion node:<br>`be[x]` where *x* is the expansion node number.<br>Compute node microprocessor:<br>`cpu[x]` where *x* is the microprocessor number.<br>Compute node memory:<br>`memory[x]` where *x* is the memory module number.<br>Compute node flash DIMM storage module:<br>`flashdimm[x]` where *x* identifies the flash DIMM storage module number.<br>Compute node add-in card:<br>`addin[x]` where *x* is the add-in card number.<br>Compute node alarm panel:<br>`tap[x]` where *x* is the alarm panel number.<br>Storage backplane:<br>`stgbkplane[x]` where *x* is the storage backplane number.<br>Storage expansion enclosure:<br>`bladeenclosure[x]` where *x* is the storage expansion enclosure number. |

*Table 48. info command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | | | I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number.<br>*(continued on next page)* |
| **Display component information** *(continued)* | | | Power supply:<br>`power[`*x*`]`<br>where *x* is the power supply bay number.<br>Rear LED card:<br>`mt[`*x*`]`<br>where *x* is the rear LED card. |
| **Display management channel path information** | Displays the management channel path information for the specified command target. The following information is returned:<br>• Channel status<br>• MAC address<br>**Note:** For I/O modules that are members of a stack, the `info -path` command option is not applicable and should be disregarded. | `info -path` | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number.<br>I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |

**Notes:**

1. This command returns vital product data (VPD) information that is unique for each command target. For some targets, additional VPD information is available when using the CMM.
2. Information returned for "Slots" is of the following format. This format applies only to information returned from the `info` command and is not used when specifying command targets.
   - `Slots:` *x* for devices that occupy one node bay, where *x* indicates the node bay.
   - `Slots:` *x-y* for devices that occupy two side-by-side node bays, where *x* indicates the left node bay and *y* indicates the right node bay.
   - `Slots:` *x:y* for multiple devices that occupy one node bay, where *x* indicates the node bay and *y* indicates the device within the node bay. Devices are numbered from bottom to top. with 1 being the lowest device and the number increasing as you move up.
   - `Slots:` *x-y:z* for multiple devices that occupy two side-by-side node bays, where *x* indicates the left node bay, *y* indicates the right node bay, and *z* indicates the device within the node bays. Devices are numbered from left to right. with 1 being on the left and the number increasing as you move to the right.
   - `Slots:` *x,y,z* for devices that occupy multiple non-contiguous node bays, where the node bay numbers are a comma-delimited list in ascending order. The list will specify a minimum of two bay numbers.

3. For compute nodes, information returned for “Name” will display a read-only name, defined by the system, followed by a user-defined name in parenthesis, if one has been specified. For example, `Name: Node 05 ( mynode5 )`.

**Example:** To view the information about the Lenovo Flex System chassis, while the chassis is set as the persistent command environment, at the `system>` prompt, type
`info`

To view the information about a compute node in bay 6, while the chassis is set as the persistent command environment, at the `system>` prompt, type
`info -T blade[6]`

To view the information about compute node 1 in a logical node grouping in bay 3, while the chassis is set as the persistent command environment, at the `system>` prompt, type
`info -T bladegroup[3]:blade[1]`

To view the information about the power module in bay 1, while the chassis is set as the persistent command environment, at the `system>` prompt, type
`info -T power[1]`

The following example shows the information that might be returned from these commands:

```
system> info
UUID: 4478 DE2F 4E66 4D8C 8509 E6A6 BEE7 F364
Manufacturer: Lenovo (CELE)
Manufacturer ID: 20301
Product ID: 336
Mach type/model: 8721FT3
Mach serial number: B080SPb
Manuf date: 1211
Hardware rev: 3.1
Part no.: 88Y6680
FRU no.: 81Y2893
FRU serial no.: btNFAGB186SP
CLEI: Not Available
CMM bays: 2
Blade bays: 14
I/O Module bays: 4
Power Module bays: 6
Blower bays: 10
Rear LED Card bays: 1
U Height of Chassis 10
Product Name: Lenovo Flex Midplane
Global ID: 9TY48MBX

system> info -T blade[6]
Name: Node 05 ( node5 )
UUID: 60C2 2B17 0C5C B060 C183 060C DB30 6108
Manufacturer: Lenovo (Not Available)
Manufacturer ID: 20301
Product ID: 361
Mach type/model: 789523X
Mach serial number: 103600B
Manuf date: Not Available
Hardware rev: 0.0
Part no.: 00E1819
FRU no.: 00E1818
FRU serial no.: 10000003600B
CLEI: Not Available
```

```
Unique ID 1: Not Available
Unique ID 2: Not Available
Unique ID 3: Not Available
Unique ID 4: Not Available
Unique ID 5: Not Available
Unique ID 6: Not Available
Unique ID 7: Not Available
Unique ID 8: Not Available
Unique ID 9: Not Available
Unique ID 10: Not Available
Unique ID 11: Not Available
Unique ID 12: Not Available
Unique ID 13: Not Available
Unique ID 14: Not Available
Unique ID 15: Not Available
Unique ID 16: Not Available
MAC Address 1: Not Available
MAC Address 2: Not Available
MAC Address 3: Not Available
MAC Address 4: Not Available
MAC Address 5: Not Available
MAC Address 6: Not Available
MAC Address 7: Not Available
MAC Address 8: Not Available
MAC Address 9: Not Available
MAC Address 10: Not Available
MAC Address 11: Not Available
MAC Address 12: Not Available
MAC Address 13: Not Available
MAC Address 14: Not Available
MAC Address 15: Not Available
MAC Address 16: Not Available
MP
        Build ID:       FW763.00 (AF763_042
        Rel date:        11/20/2015
        Rev:              1247
        Role:             Permanent
MP (pending)
        Build ID:       FW763.00 (AF763_042
        Rev:              1247
        Rel date:        11/20/12
Power On Time: Unknown

Number of Boots: 0
Product Name: Flex System p260 Compute Node
Device Description: Flex System p260
Slots: 5
Asset ID: Not Available
Product version: Not AvailableType: Compute Node (Scalable)system> info -T bladegroup[3]:blade[1]
Name: Node 03 - 01
UUID: 40BC C816 F0A3 B601 78AE CCCC CCCC CCCC
Manufacturer: Lenovo (Not Available)
Manufacturer ID: 20301
Product ID: 405
Mach type/model: 7916Z11
Mach serial number: CAR2022
Manuf date: Not Available
Hardware rev: 2.0
Part no.: 95Y3397
FRU no.: 87Y0001
FRU serial no.: 232022
```

```
CLEI: Not Available
Unique ID 1: Not Available
Unique ID 2: Not Available
Unique ID 3: Not Available
Unique ID 4: Not Available
Unique ID 5: Not Available
Unique ID 6: Not Available
Unique ID 7: Not Available
Unique ID 8: Not Available
Unique ID 9: Not Available
Unique ID 10: Not Available
Unique ID 11: Not Available
Unique ID 12: Not Available
Unique ID 13: Not Available
Unique ID 14: Not Available
Unique ID 15: Not Available
Unique ID 16: Not Available
MAC Address 1: Not Available
MAC Address 2: Not Available
MAC Address 3: Not Available
MAC Address 4: Not Available
MAC Address 5: Not Available
MAC Address 6: Not Available
MAC Address 7: Not Available
MAC Address 8: Not Available
MAC Address 9: Not Available
MAC Address 10: Not Available
MAC Address 11: Not Available
MAC Address 12: Not Available
MAC Address 13: Not Available
MAC Address 14: Not Available
MAC Address 15: Not Available
MAC Address 16: Not Available
MP
        Build ID:       1AOO33N
        Rel date:       09/14/2015
        Rev:             1.80
        Role:           Primary
MP
        Build ID:       1AOO33N
        Rel date:       09/14/2015
        Rev:             1.80
        Role:           Backup
UEFI
        Build ID:       CCE111NUS
        Rel date:       03/16/2015
        Rev:             1.00
        Role:           Primary
UEFI
        Build ID:       CCE111NUS
        Rel date:       03/16/2015
        Rev:             1.00
        Role:           Backup
DSA
        Build ID:
        Rel date:       Not Available
        Rev:
        Role:           Primary
Power On Time: 0
Number of Boots: 0
Product Name: Flex System x222 Compute Node with embedded 10Gb Virtual Fabric
```

```
Device Description: Flex System x222
Slots: 3:1
Asset ID: Not Available
Product version: Not Available
Type: Compute Node (Scalable)system> info -T power[1]
UUID: 7F75 88EE 5C7D 4EC1 A954 1CBF 9853 9B00
Manufacturer: Lenovo (EMER)
Manufacturer ID: 20301
Product ID: 304
Mach type/model: Not Available
Mach serial number: Not Available
Manuf date: 2511
Hardware rev: 75.54
Part no.: 69Y5802
FRU no.: 69Y5806
FRU serial no.: ZK128116T040
CLEI: Not Available
Power Module firmware revision: 5
Power Module Cooling Device:
        Status: ok
        Count: 2
        Speed: 44%
        Avg RPM: 8300
Product Name: Lenovo 2500 W Power Supply
Device Description: Power Supply
Slots: 1
Asset ID: Not Available
Product version: Not Available
Type: Power Module
Input voltage: 200-208 VAC
system>
```

## iocomp command

This command displays the compatibility between all compute nodes and their I/O modules. It can also display detailed interface information for an individual compute node or I/O module.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "iocomp command errors" on page 444 for a list of error messages that are specific to the iocomp command.

*Table 49. iocomp command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display compatibility between all compute nodes and I/O modules** | Displays I/O module compatibility information for all compute nodes and I/O modules. | `iocomp` | Lenovo Flex System chassis:<br>`system` |
| **Display compute node compatibility details** | Displays detailed I/O module compatibility information for the specified compute node. | `iocomp` | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |
| **Display I/O module compatibility details** | Displays detailed compatibility information for the specified I/O module. | `iocomp` | I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |

**Example:** To view I/O module compatibility information for all compute nodes and I/O modules, while CMM 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type
`iocomp -T system`

To view I/O module compatibility information for the compute node in node bay 1, while CMM 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type
`iocomp -T system:blade[1]`

To view I/O module compatibility information for the I/O module in bay 2, while CMM 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type
`iocomp -T system:switch[2]`

The following example shows the information that is returned from these commands:

```
system:mm[1]> iocomp -T system
Blades
1    xPert1          OK
2    xPert2          OK
3    Development     OK
4    Marketing      OK
5    xpert3          OK
6    Sales           OK
7    xPert4          OK
9    xPert5          OK
11   Finance         OK
12   HR               OK
13   xPert6          OK
14   xPert7          OK

I/O Modules
1    OK
2    OK
3    OK
4    OK
system:mm[1]> iocomp -T system:blade[1]
  Bay     Power         Fabric Type       Fabric on Blade   Compt
-------  -------   ----------------------  ---------------   -------
 IOM 1   On       Ethernet Switch Module  Ethernet          OK
 IOM 2   On       Ethernet Switch Module  Ethernet          OK
```

```
system:mm[1]> iocomp -T system:switch[1]
   Bay       Power    Fabric Type      Compat
----------  -------  --------------  ----------
Blade 1     On       Ethernet       OK
Blade 2     On       Ethernet       OK
Blade 3     On       Ethernet       OK
Blade 4     On       Ethernet       OK
Blade 5     Off      Ethernet       OK
Blade 6     On       Ethernet       OK
Blade 7     On       Ethernet       OK
                     n/a             No Fabric
Blade 9     On       Ethernet       OK
                     Ethernet        OK
Blade 11    On       Ethernet       OK
Blade 12    On       Ethernet       OK
Blade 13    On       Ethernet       OK
Blade 14    On       Ethernet       OK
system:mm[1]>
```

## ldapcfg command

This command sets and displays the LDAP configuration settings for the CMM.

**Note:** Certificates used by the LDAP client are managed using the `sslcfg` command (see "sslcfg command" on page 328 for information).

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "ldapcfg command errors" on page 445 for a list of error messages that are specific to the ldapcfg command.

Table 50. *ldapcfg command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display LDAP settings** | Displays the LDAP settings for the CMM. | `ldapcfg` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set LDAP security version** | Sets version of LDAP security used by the CMM.<br>**Notes:**<br>• If the version is set to v1, the following values must also be set:<br>– A group filter using the `-gf` command option.<br>– A group search attribute using the `-gsa` command option.<br>– A login permission attribute using the `-lpa` command option.<br>• If the version is set to v2, the LDAP name must also be set using the `-t` command option. | `ldapcfg -v` *version*<br>where *version* is:<br>• `v1` for old user permission model<br>• `v2` for the enhanced role-based security model<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 50. ldapcfg command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set LDAP group filter** | Sets the group filter for the CMM that can be used for authentication during LDAP server login.<br>**Note:** For a group filter to be used, LDAP security must be set to v1 using the `-v` command option. | `ldapcfg -gf "`*filter*`"`<br>where "*filter*" is a quote-delimited string of up to 511 characters in length and consists of one or more group names. The colon (:) character is used to delimit multiple group names. Leading and trailing spaces in the group name are ignored. Consecutive spaces are treated as a single space. The wildcard character (*) is not supported for security reasons. A group name can be specified as a full domain name or by using the common name (cn) portion.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set LDAP group search attribute** | Sets the group search attribute that represents groups of user IDs stored on the LDAP server.<br>On Active Directory servers, the group search attribute is typically set to "memberOf". On eDirectory servers, it is typically set to "groupMembership".<br>In an OpenLDAP server environment, users are typically assigned to groups whose objectClass equals "PosixGroup". In this case, the group search attribute identifies members of a particular PosixGroup that is typically "memberUid".<br>**Note:** For a group search attribute to be used, LDAP security must be set to v1 using the `-v` command option. | `ldapcfg -gsa "`*GSA*`"`<br>where "*GSA*" is a quote-delimited string of up to 23 characters in length that contains only letters, digits, spaces, or the following characters:<br>- ( ) + , . / : ?<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 50. ldapcfg command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set LDAP login permission attribute** | Sets the login permission attribute that is used to determine retrieve user permissions on the LDAP server.<br>**Note:** For a login permission attribute to be used, LDAP security must be set to v1 using the `-v` command option. | `ldapcfg -lpa` "*permission*" where "*permission*" is a quote-delimited string of up to 23 characters in length that contains only letters, digits, spaces, or the following characters:<br>- ( ) + , . / : ?<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set LDAP name** | Sets the LDAP name for the CMM.<br>**Note:** For an LDAP name to be used, LDAP security must be set to v2 using the `-v` command option. | `ldapcfg -t` *name*<br>where *name* is an alphanumeric string up to 63 characters in length containing any character except for angle brackets ( < and > ) and spaces.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 50. ldapcfg command (continued)*

| Function | What it does | Command | **Target** *(see paths in “Command targets” on page 6)* |
|---|---|---|---|
| **Set LDAP server discovery method** | Sets the method to use for discovering LDAP servers that provide user authentication.<br>**Notes:**<br>• If the dns method is specified, the following values must also be set:<br>– A domain name using the `-dn` command option.<br>– A forest name using the `-fn` command option.<br>• If the preconf method is specified, the following values must also be set:<br>– An LDAP server hostname or IP address using the `-i1`, `-i2`, `-i3`, and `-i4` command options.<br>– A port for each LDAP server hostname or IP address using the `-p1`, `-p2`, `-p3`, and `-p4` command options. | `ldapcfg -server` *method*<br>where *method* is:<br>• `dns` for dynamic discovery<br>• `preconf` to use an LDAP server that was manually pre-configured<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See “Commands and user authority” on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set LDAP server domain name** | Sets the search domain to use for Domain Controller (DC) dynamic discovery. | `ldapcfg -dn` *domain*<br>where *domain* is an alphanumeric string up to 255 characters in length.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See “Commands and user authority” on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set LDAP server forest name** | Sets the forest name to use for Global Catalog (GC) dynamic discovery. | `ldapcfg -fn` *forestname*<br>where *forestname* is an alphanumeric string up to 63 characters in length.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See “Commands and user authority” on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 50. ldapcfg command (continued)

| Function | What it does | Command | Target *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **First LDAP server host name or IP address - set** | Checks syntax and sets the first LDAP server host name or IP address to use for pre-configured LDAP server discovery.<br>**Note:** A port for this LDAP server hostname or IP address must be set using the `-p1` command option. | `ldapcfg -i1` *hostname/ip_ address*<br>where *hostname/ip_ address* is the first host name or IP address, up to 255 characters in length.<br>This command can only be run by users who have one or more of the following command authorities:<br>- Supervisor<br>- Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Second LDAP server host name or IP address - set** | Checks syntax and sets the second LDAP server host name or IP address to use for pre-configured LDAP server discovery.<br>**Note:** A port for this LDAP server hostname or IP address must be set using the `-p2` command option. | `ldapcfg -i2` *hostname/ip_ address*<br>where *hostname/ip_ address* is the second host name or IP address, up to 255 characters in length.<br>This command can only be run by users who have one or more of the following command authorities:<br>- Supervisor<br>- Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Third LDAP server host name or IP address - set** | Checks syntax and sets the third LDAP server host name or IP address to use for pre-configured LDAP server discovery.<br>**Note:** A port for this LDAP server hostname or IP address must be set using the `-p3` command option. | `ldapcfg -i3` *hostname/ip_ address*<br>where *hostname/ip_ address* is the third host name or IP address, up to 255 characters in length.<br>This command can only be run by users who have one or more of the following command authorities:<br>- Supervisor<br>- Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 50. ldapcfg command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Fourth LDAP server host name or IP address - set** | Checks syntax and sets the fourth LDAP server host name or IP address to use for pre-configured LDAP server discovery.<br>**Note:** A port for this LDAP server hostname or IP address must be set using the `-p4` command option. | `ldapcfg -i4` *hostname/ip_ address*<br>where *hostname/ip_ address* is the fourth host name or IP address, up to 255 characters in length.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **First LDAP server port number - set** | Sets the port number of the first LDAP server to use for pre-configured LDAP server discovery. | `ldapcfg -p1` *port*<br>where *port* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Second LDAP server port number - set** | Sets the port number of the second LDAP server to use for pre-configured LDAP server discovery. | `ldapcfg -p2` *port*<br>where *port* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 50. ldapcfg command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Third LDAP server port number - set** | Sets the port number of the third LDAP server to use for preconfigured LDAP server discovery. | `ldapcfg -p3` *port*<br>where *port* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Fourth LDAP server port number - set** | Sets the port number of the fourth LDAP server to use for preconfigured LDAP server discovery. | `ldapcfg -p4` *port*<br>where *port* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set LDAP root distinguished name** | Sets the root distinguished name for the root entry of the LDAP directory tree that is used as the base object for all searches. | `ldapcfg -rd "`*name*`"`<br>where "*name*" is up to 255 characters in length and contained within double-quotes. Names can contain any character, including spaces.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 50. ldapcfg command (continued)*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "*Command targets*" on page 6)* |
|---|---|---|---|
| **Set LDAP UID search attribute** | Sets the UID search attribute that represents the user IDs stored on the LDAP server.<br>On Active Directory servers, the UID search attribute is typically set to "sAMAccountName". On Novell eDirectory and OpenLDAP servers, it is typically set to "uid". | `ldapcfg -usa` "*UID*"<br>where "*UID*" is up to 23 characters in length and contained within double-quotes. The UID can contain only letters, numbers, spaces, and the following characters: "-", "(", ")", "+", ",", ".", "/", ":", and"?".<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set LDAP server binding method** | Sets the binding method for initial connection to the LDAP server.<br>**Notes:** If the binding method is set to cc, the following values must also be set:<br>• A UID search attribute using the `-usa` command option<br>• A client distinguished name using the `-cd` command option.<br>• A client password using the `-p` and `-cp` command options. | `ldapcfg -bm` *method*<br>where *method* is:<br>• `cc` for configured credentials<br>• `lc` for login credentials<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set LDAP server to be used for authentication only** | Enables the authentication mode to use the LDAP server for authentication only with local authorization. This automatically disables the authentication mode that uses the LDAP Server for both authentication and authorization. | `ldapcfg -aom` *state*<br>where *state* is `enabled` or `disabled`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 50. ldapcfg command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set LDAP client distinguished name** | Sets the client distinguished name (DN) for initial connection to the LDAP server.<br>**Note:** A client password must also be set using the `-p` and `-cp` command options. | `ldapcfg -cd` *domain*<br>where *domain* is an alphanumeric string up to 255 characters in length containing any character except for angle brackets ( < and > ) and spaces.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set LDAP client distinguished name password** | Sets the client distinguished name password for initial connection to the LDAP server.<br>**Note:** The passwords must be specified by both the `-p` and `-cp` command options and must match. | `ldapcfg -p` *password*<br>where *password* is an alphanumeric string up to 15 characters in length.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set (confirm) LDAP client distinguished name password** | Sets, for confirmation purposes, the client distinguished name password for initial connection to the LDAP server.<br>**Note:** The passwords must be specified by both the `-p` and `-cp` command options and must match. | `ldapcfg -cp` *password*<br>where *password* is an alphanumeric string up to 15 characters in length.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

**Example:**

To display the CMM LDAP settings, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
ldapcfg -T mm[p]
```

To enable the authentication mode to use the LDAP server for authentication only with local authorization, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
ldapcfg -aom enabled -T mm[p]
```

The following example shows the information that is returned from these two commands:

```
system> ldapcfg -T mm[p]
-server dns
 Parameters for '-server dns' configuration:
   -dn dn
   -fn fn
 Parameters for '-server preconf' configuration:
   -i1
   -p1
   -i2
   -p2
   -i3
   -p3
   -i4
   -p4

Miscellaneous Parameters:
-rd
-usa
-bm lc
-aom enabled
 Parameters for '-bm cc' configuration:
   -cd

-v v1
 Parameters for '-v v1' configuration:
   -gf
   -gsa memberOf
   -lpa
 Parameters for '-v v2' configuration:
   -t
system> ldapcfg -aom enabled -T mm[p]
OK
system>
```

## led command

This command displays and sets the LED states for a specified command target, if this command target supports the LED.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See “Common errors” on page 407 for a list of error messages that apply to all commands or “led command errors” on page 445 for a list of error messages that are specific to the led command.

*Table 51. led command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display LED states for chassis** | Displays various LED states for the chassis. | `led` | Lenovo Flex System chassis:<br>`system` |
| **Display fault LED state for chassis** | Displays fault LED state for the chassis. | `led` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Display state for compute node LEDs** | Displays the state of the compute node LEDs. | `led` | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |
| **Display state for rear LED card LEDs** | Displays the state of the rear LED card LEDs of the Lenovo Flex System chassis. | `led` | Rear LED card:<br>`mt[`*x*`]`<br>where *x* is the rear LED card. |
| **Display state for fanpack LEDs** | Displays the state of the fan pack LEDs of the Lenovo Flex System chassis. | `led` | Power supply fan pack:<br>`power[`*x*`]`<br>where *x* is the power supply (fan pack) bay number. |
| **Display state for fan logic module LEDs** | Displays the state of the fan logic module LEDs of the Lenovo Flex System chassis. | `led` | Fan logic module:<br>`fanmux[`*x*`]`<br>where *x* is the fan logic module bay number. |
| **Display state for fan module fault LED** | Displays the state of the fan module fault LED of the Lenovo Flex System chassis. | `led` | Fan module:<br>`blower[`*x*`]`<br>where *x* is the fan module bay number. |
| **Display state for I/O module LEDs** | Displays state of the LEDs for the specified I/O module. | `led` | I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |

Table 51. led command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Turn off information LED**<br>**Note:** This command option applies only to CMMs installed in a Flex System Enterpise chassis. | Turns off the information LED, that is on the Flex System Enterpise chassis and some chassis components, for the specified command target | `led -info off`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis administration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system`<br>Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number.<br>Rear LED card:<br>`mt[`*x*`]`<br>where *x* is the rear LED card. |
| **Turn off compute node information LED**<br>**Note:** This command option applies only to CMMs installed in a Lenovo Flex System Carrier-Grade chassis. | Turns off the information LED, that is on the specified compute node target in a Lenovo Flex System Carrier-Grade chassis. | `led -info off`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis administration<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |
| **Set identify LED state** | Sets the state of the identify LED, that is on the Lenovo Flex System chassis and some compute nodes and I/O modules, for the command target. | `led -loc` *state*<br>where *state* is<br>• `on`<br>• `off`<br>• `blink`<br>**Note:** A *state* of `blink` can only be used for the `system` and `mt` command targets and for the compute nodes.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis administration (for Lenovo Flex System chassis)<br>• Blade administration (for compute node)<br>• I/O module administration (for I/O modules)<br>See "Commands and user authority" on page 10 for additional | Lenovo Flex System chassis:<br>`system`<br>Rear LED card:<br>`mt[`*x*`]`<br>where *x* is the rear LED card.<br>Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number.<br>I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |

Table 51. led command (continued)

| Function | What it does | Command | **Target** *(see paths in* "Command targets*" on page 6)* |
|---|---|---|---|
| | | information. | |

**Example:**To display the LED status for the compute node in bay 2, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
led -T blade[2]
```

The following example shows the information that is returned from this command:

```
system> led -T blade[2]
Sys Brd                            off
-loc                               off
Fault LED                         off
Power LED                         blink
-info                             off
Mgmt Crd                           off
DIMM 1                             off
DIMM 4                             off
DIMM 9                             off
DIMM 12                            off
Mezz Crd0                          off

system>
```

## list command

This command displays a list of devices present within the command target. It can be used to determine the physical configuration of the Lenovo Flex System chassis, including how many CMMs are installed in the Lenovo Flex System chassis and which CMM is set as primary.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "list command errors" on page 446 for a list of error messages that are specific to the list command.

*Table 52. list command*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **View command target** | Displays the current command target. If a CMM bay is the current command target, it will be identified as primary or standby (redundant). | `list` | Any installed device. |
| **View system configuration tree** | Displays the tree structure of devices present in the Lenovo Flex System chassis, starting at the command target level. If CMM bays are part of the tree, they will be identified as primary or standby (redundant). For components that have been assigned a name, this name will be displayed next to the component bay number. | `list -l` *depth*<br>where *depth* is<br>• `all` or `a` for full tree display, starting at the command target level<br>• a number from `1` to `255` , inclusive, to display a specific number of levels below the current command target. For example, `2` displays the content of the current command target plus one level below it. | Any installed device. |

**Example:** To display a list of devices installed in the Lenovo Flex System chassis, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type
`list -l a`

(This is the command syntax that can be used to determine the primary CMM.)

The following example shows the information that is returned when the command is run on a CMM:

```
system> list -l a
system
        mm[1]     primary
        mm[2]     standby
        power[1]
        power[2]
        power[3]
        power[4]
        blower[1]
        blower[2]
        switch[1]
        switch[2]
        switch[3]
        switch[4]
        blade[1]  Accounting
                sp
                cpu[1]
                cpu[2]
        blade[2]  HR
                sp
                cpu[1]
                cpu[2]
        blade[3]  Development
                sp
                cpu[1]
        blade[4]  Marketing
                sp
```

```
               cpu[1]
               cpu[2]
        blade[5]  Sales
               sp
               cpu[1]
               cpu[2]
        blade[6]  TechSupport
               sp
               exp[2]
               cpu[1]
               cpu[3]
               cpu[4]
        mt[1]
system>
```

## monalerts command

This command displays and configures alerts that are monitored by the CMM.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "monalerts command errors" on page 446 for a list of error messages that are specific to the monalerts command.

*Table 53. monalerts command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display monitored alert states** | Displays the state of all alerts being monitored by the CMM. | `monalerts` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set state for enhanced legacy alert categories** | Enables enhanced legacy alert categories.<br>• If enhanced legacy alert categories are enabled, alerts are configured using the `monalerts` command.<br>• If enhanced legacy alert categories can not be disabled once they have been enabled. | `monalerts -ec` *state*<br>where *state* is `enabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 53. monalerts command (continued)

| Function | What it does | Command | Target (see paths in "Command targets" on page 6) |
|---|---|---|---|
| **Set monitoring state for all critical alerts** | Enables or disables monitoring of all critical alerts. | `monalerts -ca` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set monitoring state for node device critical alerts** | Enables or disables monitoring of node device critical alerts. | `monalerts -cb` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set monitoring state for I/O-module critical alerts** | Enables or disables monitoring of I/O-module critical alerts. | `monalerts -ciom` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 53. monalerts command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set monitoring state for chassis or system management critical alerts** | Enables or disables monitoring of chassis or system management critical alerts. | `monalerts -ccsm` *state*<br>where *state* is `enabled` or `disabled`.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set monitoring state for cooling device critical alerts** | Enables or disables monitoring of cooling device critical alerts. | `monalerts -ccd` *state*<br>where *state* is `enabled` or `disabled`.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set monitoring state for power supply critical alerts** | Enables or disables monitoring of power supply critical alerts. | `monalerts -cpm` *state*<br>where *state* is `enabled` or `disabled`.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 53. monalerts command (continued)

| Function | What it does | Command | Target (see paths in "Command targets" on page 6) |
|---|---|---|---|
| **Set monitoring state for all warning alerts** | Enables or disables monitoring of all warning alerts.<br>**Note:** When installed in a Lenovo Flex System Carrier-Grade chassis, this command option sets the monitoring state for major and minor events. | `monalerts -wa` *state*<br>where *state* is `enabled` or `disabled`.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set monitoring state for node device warning alerts** | Enables or disables monitoring of node device warning alerts.<br>**Note:** When installed in a Lenovo Flex System Carrier-Grade chassis, this command option sets the monitoring state for major and minor events. | `monalerts -wb` *state*<br>where *state* is `enabled` or `disabled`.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set monitoring state for I/O-module warning alerts** | Enables or disables monitoring of I/O-module warning alerts.<br>**Note:** When installed in a Lenovo Flex System Carrier-Grade chassis, this command option sets the monitoring state for major and minor events. | `monalerts -wiom` *state*<br>where *state* is `enabled` or `disabled`.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 53. monalerts command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set monitoring state for chassis or system management warning alerts** | Enables or disables monitoring of chassis or system management warning alerts.<br>**Note:** When installed in a Lenovo Flex System Carrier-Grade chassis, this command option sets the monitoring state for major and minor events. | `monalerts -wcsm` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set monitoring state for event log warning alerts** | Enables or disables monitoring of event log warning alerts.<br>**Note:** When installed in a Lenovo Flex System Carrier-Grade chassis, this command option sets the monitoring state for major and minor events. | `monalerts -wel` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set monitoring state for cooling device warning alerts** | Enables or disables monitoring of cooling device warning alerts.<br>**Note:** When installed in a Lenovo Flex System Carrier-Grade chassis, this command option sets the monitoring state for major and minor events. | `monalerts -wcd` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 53. monalerts command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set monitoring state for power supply warning alerts** | Enables or disables monitoring of power supply warning alerts.<br>**Note:** When installed in a Lenovo Flex System Carrier-Grade chassis, this command option sets the monitoring state for major and minor events. | `monalerts -wpm` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set monitoring state for all informational alerts** | Enables or disables monitoring of all informational alerts. | `monalerts -ia` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set monitoring state for node device informational alerts** | Enables or disables monitoring of node device informational alerts. | `monalerts -ib` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 53. monalerts command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set monitoring state for I/O-module informational alerts** | Enables or disables monitoring of I/O-module informational alerts. | `monalerts -iiom` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set monitoring state for chassis or system management informational alerts** | Enables or disables monitoring of chassis or system management informational alerts. | `monalerts -icsm` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set monitoring state for power state informational alerts** | Enables or disables monitoring of power state (on/off) informational alerts. | `monalerts -ipon` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 53. monalerts command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set monitoring state for inventory change informational alerts** | Enables or disables monitoring of inventory change (installed components) informational alerts. | `monalerts -iinv` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set monitoring state for event log informational alerts** | Enables or disables monitoring of event log informational alerts. | `monalerts -iel` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set monitoring state for network change informational alerts** | Enables or disables monitoring of network change informational alerts. | `monalerts -inc` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 53. monalerts command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set monitoring state for user activity informational alerts** | Enables or disables monitoring of user activity informational alerts. | `monalerts -iua` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set monitoring state for cooling device informational alerts** | Enables or disables monitoring of cooling device informational alerts. | `monalerts -icd` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set monitoring state for power supply informational alerts** | Enables or disables monitoring of power supply informational alerts. | `monalerts -ipm` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

**Example:** To enable monitoring of all critical alerts and event log warning alerts and disable monitoring of all informational alerts, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
monalerts -ca enabled -wel enabled -ia disabled -T mm[p]
```

The following example shows the information that is returned from this command:

```
system> monalerts -ca enabled -wel enabled -ia disabled -T mm[p]
OK
system>
```

## ntp command

This command configures and displays the CMM network time protocol (NTP) settings.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "ntp command errors" on page 446 for a list of error messages that are specific to the ntp command.

*Table 54. ntp command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display NTP settings** | Displays the NTP settings for the specified command target. Possible return values are:<br>• -en *state* (enabled, disabled)<br>• -i *ipaddress/hostname* (IP address or hostname of the NTP server)<br>• -f *update_frequency* (NTP update frequency, in minutes)<br>• -v3en *state* (enabled, disabled)<br>• -v3 *key_info* (NTP v3 authentication entry)<br>**Note:** Return values vary based on command target. | `ntp` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number.<br>I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |
| **Enable / disable NTP** | Enables or disables NTP for the specified command target.<br>For I/O module targets, the `ntp -en` command enables or disables transfer of NTP information from the CMM to the I/O module; it does not change the NTP state of the I/O module. | `ntp -en` *state*<br>where *state* is enabled or disabled.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number.<br>I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |
| **NTP server IP address or hostname - set** | Checks syntax and sets the IP address or hostname of the NTP server. | `ntp -i` *ipaddress/ hostname*<br>where *ipaddress/ hostname* is the IP address or hostname of the NTP server.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 54. ntp command (continued)*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **NTP update frequency - set** | Sets how often the clock in the specified command target is automatically updated by the NTP server. | `ntp -f` *time*<br>where *time* is the NTP update frequency, in minutes with a maximum value of 45000.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number.<br>I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |
| **NTP - Enable / disable V3 authentication** | Enables or disables V3 authentication between the CMM and the NTP server.<br>**Note:** The NTP server authentication key must be set, using the ntp -v3 command option, before enabling V3 authentication. | `ntp -v3en` *state*<br>where *state* is `enabled` or `disabled`.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 54. ntp command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **NTP server authentication key - set** | Sets the v3 authentication key that the CMM uses to access the NTP server. The authentication key contains the following values:<br>• Key index: An NTP server can be configured with one or more key entries. The key index specifies which key the server expects the client to authenticate with.<br>• Key type: The CMM supports only the SHA1 key type.<br>• Key: The key is an 40-character ASCII string.<br>• The `ntp -v3`*key_index* and *key* values must match the "key ID" and "password" values set on the NTP server. See the documentation for your NTP server for information about setting a key ID and password. | `ntp -v3` *key_indexkey_typekey*<br>where:<br>• *key_index* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.<br>• *key_type* is `SHA1`.<br>• *key* is a 40-character ASCII string.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **NTP clock-synchronize** | Synchronizes the CMM clock with the NTP server. (You must configure a valid NTP server before you can synchronize.) | `ntp -synch`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

**Example:**

To display NTP settings for the CMM, while the primary CMM in bay 2 is set as the persistent command environment, at the `system:mm[2]>` prompt, type
`ntp`

The following example shows the information that is returned from this command:

```
system:mm[2]> ntp
-en enabled
-i timeserver
-f 5
-v3en disabled
-v3 Not configured
NTP is disabled.
system:mm[2]>
```

## permgroups command

This command displays and configures user permission groups of the primary CMM.

**Important:** Users and permission groups for the Lenovo Flex System chassis are controlled by the CMM in each Lenovo Flex System chassis, using the CMM CLI "users command" on page 372 and the "permgroups command" on page 238 or the CMM web interface. If your Lenovo Flex System configuration includes an optional management device, such as the Lenovo XClarity Administrator or Flex System Manager hardware, users and permission groups for each optional management device installation are controlled by the optional management device software (see http://flexsystem.lenovofiles.com/help/topic/com.lenovo.lxca.doc/aug_product_page.html for information about Lenovo XClarity Administrator or see http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.8731.doc/product_page.html for information about the Flex System Manager).

**Notes:**

- Permission groups are assigned to users using the "users command" on page 372.
- Permission groups can be backed up as part of the CMM configuration using the "write command" on page 404.
- Permission groups are restored as part of a backed up CMM configuration using the "read command" on page 280.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "permgroups command errors" on page 447 for a list of error messages that are specific to the permgroups command.

*Table 55. permgroups command*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display all user permission groups** | Displays all user permission groups set up for the CMM. | `permgroups` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Display specific user permission group** | Displays information for the specified user permission group. | `permgroups -n` *group_name*<br>where *group_name* is the name that identifies the user permission group. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 55. permgroups command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Add user permission group** | Creates a new user permission group.<br>**Notes:**<br>• User permission group names can not be changed after they are added.<br>• Group names are not case sensitive. | `permgroups -add -n` *group_name* `-a` *group_authority*<br>where:<br>• *group_name* is an alphanumeric string up to 63 characters in length that can include periods ( . ) and underscores ( _ ). Each group name must be unique. Group names are not case sensitive.<br>• *group_authority* uses the following syntax:<br>– `operator` (Operator)<br>– `rbs:`*roles*`:`*scope* where the *roles* are one or more of the following authority levels, separated by a vertical bar ( \| ):<br>– `super` (Supervisor)<br>– `cam` (Chassis User Account Management)<br>– `clm` (Chassis Log Management)<br>– `co` (Chassis Operator)<br>– `cc` (Chassis Configuration)<br>– `ca` (Chassis Administration)<br>– `bo` (Blade Operator)<br>– `brp` (Blade Remote Present)<br>– `bc` (Blade Configuration)<br>– `ba` (Blade Administration)<br>– `so` (I/O Module Operator)<br>– `sc` (I/O Module Configuration)<br>– `sa` (I/O Module Administration)<br>*(continued on next page)* | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Add user permission group** *(continued)* |  | where the *scope* is one or more of the following devices, separated by a vertical bar ( \| ). Ranges of devices are separated by a dash ( - ). |  |

*Table 55. permgroups command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | | - `c` *n* (Chassis *n*, where *n* is 1)<br>- `b` *n* (Blade *n*, where *n* is a valid node bay number in the chassis)<br>- `s` *n* (I/O module *n*, where *n* is a valid I/O-bay number in the chassis)<br><br>This command can only be run by users who have one or more of the following command authorities:<br>- Supervisor<br>- Chassis account management<br>See "Commands and user authority" on page 10 for additional information. | |
| **Modify user permission group** | Modify the selected user permission group.<br>**Notes:**<br>- User permission group names can not be changed after they are added.<br>- Group names are not case sensitive. | `permgroups -n` *group_name* `-a` *group_authority*<br>where:<br>- *group_name* is the name that identifies the user permission group.<br>- *group_authority* uses the following syntax:<br>– `operator` (Operator)<br>– `rbs:`*roles*`:`*scope* where the *roles* are one or more of the following authority levels, separated by a vertical bar ( \| ):<br>– `super` (Supervisor)<br>– `cam` (Chassis User Account Management)<br>– `clm` (Chassis Log Management)<br>– `co` (Chassis Operator)<br>– `cc` (Chassis Configuration)<br>– `ca` (Chassis Administration)<br>– `bo` (Blade Operator)<br>– `brp` (Blade Remote Present)<br>– `bc` (Blade Configuration) | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 55. permgroups command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | | – `ba` (Blade Administration)<br>– `so` (I/O Module Operator)<br>– `sc` (I/O Module Configuration)<br>– `sa` (I/O Module Administration)<br>*(continued on next page)* | |
| **Modify user permission group** *(continued)* | | where the *scope* is one or more of the following devices, separated by a vertical bar ( \| ). Ranges of devices are separated by a dash ( - ).<br>• `c` *n* (Chassis *n*, where *n* is 1)<br>• `b` *n* (Blade *n*, where *n* is a valid node bay number in the chassis)<br>• `s` *n* (I/O module *n*, where *n* is a valid I/O-bay number in the chassis)<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>See "Commands and user authority" on page 10 for additional information. | |
| **Delete user permission group** | Delete the specified user permission group.<br>**Note:** Group names are not case sensitive. | `permgroups -n` *group_name* `-clear`<br>where *group_name* is the name that identifies the user permission group.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

**Example:** To add a user permission group with a name of superuser that has supervisor rights to all Lenovo Flex System components, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
permgroups -add -n superuser -a rbs:super:c1|b1-b14|s1-s4 -T mm[p]
```

To display information for the superuser group, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
permgroups -n superuser -T mm[p]
```

The following example shows the information that is returned from these commands:

```
system> permgroups -add -n superuser -a rbs:super:c1|b1-b14|s1-s4 -T mm[p]
OK
system> permgroups -n superuser -T mm[p]

-a Role:supervisor
   Blades:1|2|3|4|5|6|7|8|9|10|11|12|13|14
   Chassis:1
   Modules:1|2|3|4

system>
```

## ping command

This command tests the internal communication path between the CMM and an Lenovo Flex System component by sending it a ping request.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "ping command errors" on page 449 for a list of error messages that are specific to the ping command.

*Table 56. ping command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display IP addresses** | Displays a list of index numbers and IP addresses for the specified command target. | `ping -i` | Compute node:<br>`blade[x]` where *x* is the node bay number.<br>I/O module:<br>`switch[x]` where *x* is the I/O-bay number. |
| **Ping compute node IP address** | Pings the specified compute node IP address to test communication between the compute node and the CMM. | `ping -i` *ip_address* where *ip_address* is the IP address to ping.<br>**Note:** Valid index numbers and IP addresses for components installed in the Lenovo Flex System chassis can be seen by running the `ping -i` command, directed to a specific command target with no arguments. | Compute node:<br>`blade[x]` where *x* is the node bay number. |
| **Ping I/O-module IP address** | Pings the specified I/O-module IP address to test communication between the I/O module and the CMM. | I/O module:<br>`switch[x]` where *x* is the I/O-bay number. | |

*Table 56. ping command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Ping compute node IP address** | Pings the specified compute node to test communication. | `ping -i` *index*<br>where *index* is the index number for the compute node IP address to ping.<br>**Note:** Valid index numbers and IP addresses for components installed in the Lenovo Flex System chassis can be seen by running the `ping -i` command, directed to a specific command target with no arguments. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |
| **Ping I/O-module IP address** | Pings the specified I/O module to test communication. | `ping -i` *index*<br>where *index* is the index number for the I/O-module IP address to ping.<br>**Note:** Valid index numbers and IP addresses for components installed in the Lenovo Flex System chassis can be seen by running the `ping -i` command, directed to a specific command target with no arguments. | I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |

**Example:** To display the IP addresses of the I/O module in bay 2, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
ping -T switch[2] -i
```

To ping the second IP address of the I/O module in bay 2 using an index number, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
ping -T switch[2] -i 2
```

To ping the second IP address of the I/O module in bay 2 using an IP address, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
ping -T switch[2] -i fe80::a17:f4ff:fe89:a9ef
```

The following example shows the information that is returned from these commands:

```
system> ping -T switch[2] -i
1. 192.168.70.121
2. fe80::a17:f4ff:fe89:a9ef
3. 3000:1013::a17:f4ff:fe89:a9ef
4. 3001:1013::a17:f4ff:fe89:a9ef
5. 3002:1013::a17:f4ff:fe89:a9ef
6. 2000:1013::a17:f4ff:fe89:a9ef
7. 2001:1013::a17:f4ff:fe89:a9ef
8. 2002:1013::a17:f4ff:fe89:a9ef
```

```
system> ping -T switch[2] -i 2
Reply from fe80::a17:f4ff:fe89:a9ef: bytes=16384 time=201850.880ms
Reply from fe80::a17:f4ff:fe89:a9ef: bytes=16384 time=3120824.320ms
Reply from fe80::a17:f4ff:fe89:a9ef: bytes=16384 time=2953052.160ms
Reply from fe80::a17:f4ff:fe89:a9ef: bytes=16384 time=33685.504ms
system> ping -T switch[2] -i fe80::a17:f4ff:fe89:a9ef
Reply from fe80::a17:f4ff:fe89:a9ef: bytes=16384 time=1912799.232ms
Reply from fe80::a17:f4ff:fe89:a9ef: bytes=16384 time=922877.952ms
Reply from fe80::a17:f4ff:fe89:a9ef: bytes=16384 time=2281963.520ms
Reply from fe80::a17:f4ff:fe89:a9ef: bytes=16384 time=4060282.880ms
system>
```

## pmpolicy command

This command displays and sets the power management policies for the Lenovo Flex System chassis.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See “Common errors” on page 407 for a list of error messages that apply to all commands or “pmpolicy command errors” on page 449 for a list of error messages that are specific to the pmpolicy command.

Table 57. *pmpolicy command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display current power management policy** | Displays the current power management policy. | `pmpolicy` | Lenovo Flex System chassis:<br>`system` |
| **Display current and available power management policies** | Displays both the current and available power management policies. | `pmpolicy pd` | Lenovo Flex System chassis:<br>`system` |
| **Set power management policy** | Set power management policy. | `pmpolicy -pm` *policy*<br>or<br>`pmpolicy pd -pm` *policy*<br>where *policy* is:<br>• `acred` (ac power source redundancy policy)<br>• `acredov` (ac power source redundancy policy, with compute node throttling)<br>• `redwoperf` (power supply redundancy, no compute node oversubscription)<br>• `redwperf` (power supply redundancy with compute node power throttling)<br>• `nonred` (no power management policy)<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system` |

**Example:**

To view the current power management policy, while the primary CMM in bay 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
pmpolicy -T system
```

The following example shows the output generated by this command.

```
system:mm[1]> pmpolicy -T system
```

```
Power Domain
--------------

Power Management Policy:
        Basic Power Management (nonred)
Description:
        Total allowed power is higher than other policies and is limited only
        by the total power capacity of all the Power Modules up to the
        maximum of chassis power rating. This is the least conservative
        approach, since it does not provide any protection for power source
        or Power Module failure. If any single power supply fails, blade
        and/or chassis operation may be affected.
Power Supply Failure Limit:       0
Maximum Power Limit (Watts):   5490
Your Estimated Utilization:      20%

NOTE:
 Power Supply Failure Limit: This is the maximum number of power supplies
                             that can fail while still guaranteeing the
                             operation of the domain in the selected policy.
 Your Estimated Utilization: The estimated utilization is based on the maximum
                             power limit allowed in this policy and the current
                             aggregated power in use of all components in the
                             domain.

system:mm[1]>
```

## portcfg command

This command configures and displays the settings for the CMM serial port.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See “Common errors” on page 407 for a list of error messages that apply to all commands or “portcfg command errors” on page 449 for a list of error messages that are specific to the portcfg command.

*Table 58. portcfg command*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display CMM serial port configuration** | Displays the current configuration of the CMM serial port. Possible return values are:<br>• -b *baud_rate*<br>• -p *parity*<br>• -s *stop_bits* | `portcfg -com1` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set CMM serial port baud rate** | Checks syntax and sets the baud (communications) rate of the CMM serial port. | `portcfg -com1 -b` *baud_rate*<br>where *baud_rate* is 2400, 4800, 9600, 19200, 38400, 57600, or 115200.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 58. portcfg command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set CMM serial port parity** | Checks syntax and sets the parity of the CMM serial port. | `portcfg -com1 -p` *parity*<br>where *parity* is<br>• `none`<br>• `odd`<br>• `even`<br>• `mark`<br>• `space`<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set CMM serial port stop bits** | Checks syntax and sets the number of stop bits for the CMM serial port.<br>**Note:** When `2` stop bits is selected, the software automatically adjusts between 1.5 and 2 stop bits, based on the detected data-word size. | `portcfg -com1 -s` *stop_bits*<br>where *stop_bits* is:<br>• `1` for 1 stop bit.<br>• `2` for 1.5 or 2 stop bits.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

**Example:**

To display the configuration for the CMM serial port, while the primary CMM in bay 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type
`portcfg -com1`

To set the baud rate for the CMM serial port to 9600, while the primary CMM in bay 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type
`portcfg -com1 -b 9600`

The following example shows the information that is returned from these two commands:

```
system:mm[1]> portcfg -com1
-b 2400
-p none
-s 1
system:mm[1]> portcfg -com1 -b 9600
These configuration changes will become active after the next reset of the MM.
```

```
system:mm[1]>
```

## ports command

This command sets and displays the network port configuration settings for the CMM and I/O modules.

**Notes:**

- Changes to the `-ftpe`, `-snmp1ae`, `-snmp3ae`, `-snmpte`, `-sshe`, `-ftpp`, `-ftpdp`, `-httpp`, `-httpsp`, `-snmpap`, `-snmptp`, `-sshp`, `-tcme`, `-telnete`, `-telnetp`, `-telnett`, or `-tftpp` settings become active immediately. Changes to the remaining settings become active after the next reset of the CMM.
- The CMM HTTP and HTTPS ports are open at all times. Port behavior is determined by the CMM HTTPS port setting, which can be affected by the CMM chassis security policy setting:
  - When the CMM HTTPS port is enabled, the HTTP port (port 80) remains open and redirects to the HTTPS port (port 443). When the chassis security policy is set to secure, the CMM HTTPS port is automatically enabled and its setting cannot be changed.
  - When the CMM HTTPS port is disabled, the HTTPS port (port 443) remains open and redirects to the HTTP port (port 80).

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "ports command errors" on page 450 for a list of error messages that are specific to the ports command.

*Table 59. ports command*

| **Function** | **What it does** | **Command** | **Target** *(see paths in “Command targets” on page 6)* |
|---|---|---|---|
| **Display network port settings** | Displays the network port settings for the CMM. Returned values are:<br>• -cimp *cim_prt_num*<br>• -ftpp *FTP_prt_num*<br>• -ftpdp *FTP_data_prt_num*<br>• -httpp *HTTP_prt_num*<br>• -httpsp *HTTPS_prt_num*<br>• -slpp *SLP_prt_num*<br>• -snmpap *SNMP_agent_prt_num*<br>• -snmptp *SNMP_traps_prt_num*<br>• -sshp *SSH_prt_num*<br>• -stcmp *secure_tcmp*<br>• -tcmp *TCP_cmd_md_port*<br>• -telnetp *_Telnet_prt_num*<br>• -tftpp *TFTP_prt_num*<br>• -cime *cim_prt_state*<br>• -ftpe *FTP_state*<br>• -sftpe *sec_FTP_state*<br>• -httpse *HTTPS_prt_state*<br>• -ntpe *NTP_state*<br>• -slpe *SLP_state*.<br>• -snmp1ae *SNMPv1_agent_state*<br>• -snmp3ae *SNMPv3_agent_state*<br>• -snmpte *SNMP_traps_state*<br>• -sshe *SSH_prt_state*<br>• -stcme *secure_TCP_cmd_mode*<br>• -tcme *TCP_cmd_mode_state*<br>• -telnete *Telnet_prt_state-*<br>• -tftpe *TFTP_state*<br>• -ftpt *FTP_timeout*<br>• -tcmt *TCP_cmd_mode_timeout*<br>• -telnett *Telnet_prt_timeout*<br>**Notes:**<br>• The following will not be available if the CMM chassis security level is set to secure with the “security command” on page 298:<br>– HTTP<br>– FTP<br>– SNMPv1<br>– Telnet<br>– TFTP<br>– Non-secure TCP command mode<br>• HTTPSE can only be disabled by disabling all web access using the “uicfg command” on page 357. | `ports` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Display open CMM ports** | Displays the CMM ports that are currently open.<br>**Notes:** The following will not be available if the CMM security level is set to secure with the “security command” on page 298:<br>• HTTP | `ports -open` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]` |

Table 59. ports command (continued)

| Function | What it does | Command | Target (see paths in "Command targets" on page 6) |
|---|---|---|---|
| | • FTP<br>• SNMPv1<br>• Telnet<br>• TFTP<br>• Non-secure TCP command mode | | where x is the primary CMM bay number. |
| **Reset network port settings** | Resets all network port settings for the CMM to the default values. Default values are:<br>• -ftpp: 21<br>• -ftpdp: 20<br>• -cimp: 5989<br>• -httpp: 80<br>• -httpsp: 443<br>• -slpp: 427<br>• -tcmp: 6090<br>• -snmpap: 161<br>• -snmptp: 162<br>• -sshp: 22<br>• -stcmp: 6091<br>• -telnetp: 23<br>• -tftpp: 69<br>**Notes:** The following will not be available if the CMM security level is set to secure with the "security command" on page 298:<br>• HTTP<br>• FTP<br>• SNMPv1<br>• Telnet<br>• TFTP<br>• Non-secure TCP command mode | `ports -reset`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set FTP port number** | Sets the port number for the CMM FTP port.<br>**Notes:**<br>• The FTP port will not be available if the CMM chassis security level is set to secure with the "security command" on page 298.<br>• You cannot configure a port to a number that is already in use.<br>• Changes to port numbers take effect immediately.<br>• Changing port numbers will affect ongoing operations using the service at that port. | `ports -ftpp` *FTP_prt_num*<br>where *FTP_prt_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 59. ports command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set FTP data port number** | Sets the port number for the CMM FTP data port.<br>**Notes:**<br>• The FTP data port will not be available if the CMM chassis security level is set to secure with the "security command" on page 298.<br>• You cannot configure a port to a number that is already in use.<br>• Changes to port numbers take effect immediately.<br>• Changing port numbers will affect ongoing operations using the service at that port. | `ports -ftpdp` *FTP_data_prt_num*<br>where *FTP_data_prt_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set HTTP port number** | Sets the port number for the CMM HTTP port.<br>**Notes:**<br>• The HTTP port will not be available if the CMM security level is set to secure with the "security command" on page 298.<br>• You cannot configure a port to a number that is already in use.<br>• Changes to port numbers take effect immediately.<br>• Changing port numbers will affect ongoing operations using the service at that port. | `ports -httpp` *HTTP_prt_num*<br>where *HTTP_prt_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set HTTPS port number** | Sets the port number for the CMM HTTPS port.<br>**Notes:**<br>• You cannot configure a port to a number that is already in use.<br>• Changes to port numbers take effect immediately.<br>• Changing port numbers will affect ongoing operations using the service at that port. | `ports -httpsp` *HTTPS_prt_num*<br>where *HTTPS_prt_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 59. ports command (continued)

| Function | What it does | Command | Target (see paths in "Command targets" on page 6) |
|---|---|---|---|
| **Set CIM port number over HTTPS** | Sets the port number for using the CMM common information model (CIM) over HTTPS.<br>**Notes:**<br>• You cannot configure a port to a number that is already in use.<br>• Changes to port numbers take effect immediately.<br>• Changing port numbers will affect ongoing operations using the service at that port. | `ports -cimp` *cim_prt_num*<br>where *cim_prt_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set SLP port number** | Sets the SLP port number.<br>**Notes:**<br>• You cannot configure a port to a number that is already in use.<br>• Changes to port numbers take effect immediately.<br>• Changing port numbers will affect ongoing operations using the service at that port. | `ports -slpp` *SLP_prt_num*<br>where *SLP_prt_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set SNMP agent port number** | Sets the port number for the CMM SNMP agent port.<br>**Notes:**<br>• SNMPv1 ports will not be available if the CMM security level is set to secure with the "security command" on page 298.<br>• You cannot configure a port to a number that is already in use.<br>• Changes to port numbers take effect immediately.<br>• Changing port numbers will affect ongoing operations using the service at that port. | `ports -snmpap` *SNMP_agent_prt_num*<br>where *SNMP_agent_prt_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 59. ports command (continued)*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set SNMP traps port number** | Sets the port number for the CMM SNMP traps port.<br>**Notes:**<br>• SNMPv1 ports will not be available if the CMM security level is set to secure with the "security command" on page 298.<br>• You cannot configure a port to a number that is already in use.<br>• Changes to port numbers take effect immediately.<br>• Changing port numbers will affect ongoing operations using the service at that port. | `ports -snmptp` *SNMP_traps_prt_num*<br>where *SNMP_traps_prt_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set command mode port number** | Sets the TCP command mode port number.<br>**Important:** The optional Flex System Manager software requires this port to be 6090.<br><br>**Notes:**<br>• Non-secure TCP command mode ports will not be available if the CMM security level is set to secure with the "security command" on page 298.<br>• You cannot configure a port to a number that is already in use.<br>• Changes to port numbers take effect immediately.<br>• Changing port numbers will affect ongoing operations using the service at that port. | `ports -tcmp` *TCP_cmd_md_prt_num*<br>where *TCP_cmd_md_prt_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 59. ports command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set secure command mode port number** | Sets the secure TCP command mode port number.<br>**Notes:**<br>• You cannot configure a port to a number that is already in use.<br>• Changes to port numbers take effect immediately.<br>• Changing port numbers will affect ongoing operations using the service at that port. | `ports -stcmp` *secure_tcmp*<br>where *secure_tcmp* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set SSH port number** | Sets the port number for the CMM SSH port.<br>**Notes:**<br>• You cannot configure a port to a number that is already in use.<br>• Changes to port numbers take effect immediately.<br>• Changing port numbers will affect ongoing operations using the service at that port. | `ports -sshp` *SSH_prt_num*<br>where *SSH_prt_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set Telnet port number** | Sets the port number for the CMM Telnet port.<br>**Notes:**<br>• The Telnet port will not be available if the CMM chassis security level is set to secure with the "security command" on page 298.<br>• You cannot configure a port to a number that is already in use.<br>• Changes to port numbers take effect immediately.<br>• Changing port numbers will affect ongoing operations using the service at that port. | `ports -telnetp` *Telnet_prt_num*<br>where *Telnet_prt_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 59. ports command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set TFTP port number** | Sets the port number for the CMM TFTP port.<br>**Notes:**<br>• The TFTP port will not be available if the CMM security level is set to secure with the "security command" on page 298.<br>• You cannot configure a port to a number that is already in use.<br>• Changes to port numbers take effect immediately.<br>• Changing port numbers will affect ongoing operations using the service at that port. | `ports -tftpp` *TFTP_prt_num*<br>where *TFTP_prt_num* is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Enable / disable FTP** | Enables or disables FTP for the CMM.<br>**Note:** The FTP port can not be enabled if the CMM chassis security level is set to secure with the "security command" on page 298. | `ports -ftpe` *state*<br>where *state* is `on` or `off` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Enable / disable SFTP** | Enables or disables secure FTP for the CMM. | `ports -sftpe` *state*<br>where *state* is `on` or `off` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 59. ports command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Enable / disable HTTPS port** | Enables or disables the CMM HTTPS port.<br>**Note:** Disabling the HTTPS port automatically enables HTTP. | `ports -httpse` *state*<br>where *state* is `on` or `off` .<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Enable / disable CIM over HTTPS** | Enables or disables CIM over HTTPS for the CMM. | `ports -cime` *state*<br>where *state* is `on` or `off` .<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Enable / disable NTP** | Enables or disables NTP for the CMM. | `ports -ntpe` *state*<br>where *state* is `on` or `off` .<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Enable / disables SLP** | Enables or disables SLP for the CMM. | `ports -slpe` *state*<br>where *state* is `on` or `off` .<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 59. ports command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Enable / disable SNMPv1 agent** | Enables or disables the SNMPv1 agent for the CMM.<br>**Note:** The SNMPv1 agent can not be enabled if the CMM chassis security level is set to secure with the "security command" on page 298. | `ports -snmp1ae` *state*<br>where *state* is `on` or `off` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Enable / disable SNMPv3 agent** | Enables or disables the SNMPv3 agent for the CMM. | `ports -snmp3ae` *state*<br>where *state* is `on` or `off` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Enable / disable SNMP traps** | Enables or disables the SNMP traps for the CMM. | `ports -snmpte` *state*<br>where *state* is `on` or `off` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Enable / disable SSH port** | Enables or disables the CMM SSH port. | `ports -sshe` *state*<br>where *state* is `on` or `off` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 59. ports command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Enable / disable TCP command mode and set number of connections** | Turns the TCP command mode on or off, or sets the maximum number of connections explicitly.<br>**Notes:**<br>• Any number of connections (1 through 20) displays a status of on. Zero connections displays a status of off.<br>• Non-secure TCP command mode can not be enabled if the CMM chassis security level is set to secure with the "security command" on page 298.<br>• The total session count of TCM and STCM is limited to 20. | `ports -tcme` *port_mode*<br>where *port_mode* is `on` (1 connection), `off` (no connections), or a number between 0 and 20, inclusive, that indicates the maximum number of TCP session connections.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Enable / disable secure TCP command mode and set number of connections** | Turns the secure TCP command mode on or off, or sets the maximum number of connections.<br>**Notes:**<br>• On a write operation, the maximum number of connections can be set explicitly (0-20), or it can be turned on (1 connection) or off (0 connections).<br>• On a read operation, off means 0 connections, and on means 1 or more connections.<br>• The total session count of TCM and STCM is limited to 20. | `ports -stcme` *port_mode*<br>where *port_mode* is `on` (1 connection), `off` (no connections), or a number between 0 and 20, inclusive, that indicates the maximum number of TCP session connections.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Enable / disable Telnet port** | Enables or disables the CMM Telnet port.<br>**Note:** Telnet can not be enabled if the CMM chassis security level is set to secure with the "security command" on page 298. | `ports -telnete` *state*<br>where *state* is `on` or `off` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 59. ports command (continued)*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Enable / disable TFTP** | Enables or disables TFTP for the CMM.<br>**Note:** TFTP can not be enabled if the CMM security level is set to secure with the "security command" on page 298. | `ports -tftpe` *state*<br>where *state* is `on` or `off` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set FTP timeout** | Sets the FTP timeout value for the CMM. | `ports -ftpt` *timeout*<br>where *timeout* is from 0 seconds (no timeout) to 4294967295 seconds, inclusive.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set TCP command-mode timeout** | Sets the TCP command-mode timeout value for the CMM. | `ports -tcmt` *timeout*<br>where *timeout* is from 0 seconds (no timeout) to 4294967295 seconds, inclusive.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 59. ports command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set Telnet port timeout** | Sets the Telnet port timeout value for the CMM. | `ports -telnett` *timeout*<br>where *timeout* is from 0 seconds (no timeout) to 4294967295 seconds, inclusive.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Display network port settings for I/O module** | Displays the network port settings for the I/O module. These settings can include:<br>• cable compatibility<br>• cable length<br>• cable type<br>• data rate<br>• label<br>• port index<br>• port media<br>• port width<br>• protocol<br>• speed<br>• speed setting<br>• available speeds<br>• state<br>• state setting<br>• type<br>• vendor<br>**Note:** Other device specific values might be returned. | `ports` | I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |

*Table 59. ports command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Enable or disable port for I/O module** | Enables or disables specified port on specified I/O module. | `ports` -*port_index* `-state` *state*<br>where<br>• *port_index* is from 1 to 65535, inclusive.<br>• *state* is `on` or `off` .<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• I/O module configuration<br>See "Commands and user authority" on page 10 for additional information. | I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |
| **Sets speed of port for I/O module** | Sets speed of specified port on I/O modules that support this feature. | `ports` -*port_index* `-speed` *speed_setting*<br>where<br>• *port_index* is from 1 to 65535, inclusive.<br>• *speed_setting* specifies the port speed, in terms of:<br>– *multiplier*<br>– *units*, `m` or `g` for megabits or gigabits<br>– *duplex mode*, `h` or `f` for half or full<br>For example:<br>– `100mh` sets the port speed to 100 Mbps half-duplex.<br>– `10gf` sets the port speed to 10 Gbps full-duplex.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• I/O module configuration<br>See "Commands and user authority" on page 10 for additional information. | I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |

**Example:**

To display the CMM network port settings, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
ports -T mm[p]
```

To disable FTP for the CMM, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
ports -ftpe off -T mm[p]
```

The following example shows the information that is returned from these commands:

```
system> ports -T mm[p]
-cimp 5989
-ftpp 21
-ftpdp 20
-httpp 80
-httpsp 443
-slpp 427
-snmpap 161
-snmptp 162
-sshp 22
-stcmp 6091
-tcmp 6090
-telnetp 23
-tftpp 69
-cime on
-ftpe off
-httpse on
-ntpe off
-sftpe on
-slpe on
-snmp1ae on
-snmp3ae on
-snmpte on
-sshe on
-stcme off
-tcme on
-telnete off
-tftpe off
-tcmt 300
-telnett 300
-ftpt 300
system> ports -ftpe off -T mm[p]
Changes to -sshe, -sshp, -telnetp, -telnete,
-telnett, -snmpte, -tcme, -tcmp, -tcmt, -stcme, -stcmp,
-httpp,-httpse, -httpsp, -ftpe or -tftpe will become active immediately.
OK
system>
```

## power command

This command turns on and turns off compute nodes and I/O modules.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "power command errors" on page 452 for a list of error messages that are specific to the power command.

Table 60. power command

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Power on** | Turns on the specified command target.<br>**Note:** Some storage nodes might have specific boot sequence requirements, see the documentation for your storage node for details. | `power -on`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade administration (for compute node)<br>• I/O module administration (for I/O module)<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number.<br>I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |
| **Power on to command console** | Opens a command console with an SOL session when the specified compute node is turned on.<br>**Note:** Some storage nodes might have specific boot sequence requirements, see the documentation for your storage node for details. | `power -on -c`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade administration and blade remote presence<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |
| **Enable / disable SMS for compute node** | Enable or disable the System Management Services (SMS) firmware menu on the specified compute node, for compute nodes that support this feature.<br>**Notes:**<br>• The compute node will restart immediately after setting the -sms option.<br>• The -sms option state that is set is retained after the compute node restarts.<br>• The -f1, -f2-sms, -wol, -local, -ap, and -d command options can be entered together, but these options must be used exclusive of all other command options. | `power -sms` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade administration<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |

*Table 60. power command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Enable / disable F1 (Setup) for compute node** | Enable or disable F1 (Setup) menu on the specified compute node, for compute nodes that support this feature.<br>**Notes:**<br>• The compute node will restart immediately after setting the -f1 option.<br>• The -f1 option state that is set is retained after the compute node restarts.<br>• The -f1, -f2, -sms, -wol, -local, -ap, and -d command options can be entered together, but these options must be used exclusive of all other command options. | `power -f1` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade administration<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |
| **Enable / disable F2 (Diagnostics) for compute node** | Enable or disable F2 (Diagnostics) menu on the specified compute node, for compute nodes that support this feature.<br>**Notes:**<br>• The compute node will restart immediately after setting the -f2 option.<br>• The -f2 option state that is set is retained after the compute node restarts.<br>• The -f1, -f2, -sms, -wol, -local, -ap, and -d command options can be entered together, but these options must be used exclusive of all other command options. | `power -f2` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade administration<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |
| **Power off** | Turns off the specified command target. | `power -off`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade administration (for compute node)<br>• I/O module administration (for I/O module)<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number.<br>I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |

Table 60. power command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Shutdown and power off compute node** | Shuts down the operating system and turns off the specified compute node. | `power -softoff`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade administration<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |
| **Power cycle** | Cycles power for the specified compute node or I/O module. If the compute node or I/O module is off, it will turn on. If the compute node or I/O module is on, it will turn off and then turn on. | `power -cycle`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade administration (for compute node)<br>• I/O module administration (for I/O module)<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number.<br>I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |
| **Power cycle to command console** | Cycles power for the specified compute node. If the compute node is off, it opens a command console with an SOL session when it is turned on. If the compute node is on, it will turn off and then turn on. | `power -cycle -c`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade administration and blade remote presence<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |
| **Display power state** | Displays the current power state for the specified compute node or I/O module. Possible return values are off, on, standby, or hibernate. | `power -state` | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number.<br>I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |

*Table 60. power command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Enable / disable Wake on LAN globally** | Enables or disables Wake on LAN globally for all compute nodes.<br>**Note:** The -wol, -sms, -local, -ap, and -d command options can be entered together, but these options must be used exclusive of all other command options. | `power -wol` *state*<br>where *state* is `enabled` or `disabled`.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system` |
| **Enable / disable Wake on LAN for compute node** | Enables or disables Wake on LAN for the specified compute node.<br>**Note:** The -wol, -sms,-local, -ap, and -d command options can be entered together, but these options must be used exclusive of all other command options. | `power -wol` *state*<br>where *state* is `enabled` or `disabled`.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade configuration<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |
| **Enable / disable local power control globally** | Enables or disables local power control globally for all compute nodes.<br>**Note:** The -local, -sms, -wol, -ap, and -d command options can be entered together, but these options must be used exclusive of all other command options. | `power -local` *state*<br>where *state* is `enabled` or `disabled`.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system` |

Table 60. power command (continued)

| Function | What it does | Command | Target (see paths in "Command targets" on page 6) |
|---|---|---|---|
| **Enable / disable local power control for compute node** | Enables local power control for the specified compute node.<br>**Note:** The -local, -sms, -wol, -ap, and -d command options can be entered together, but these options must be used exclusive of all other command options. | `power -local` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade configuration<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |
| **Set automatic power-on policy for compute node** | Sets the automatic power-on policy for the targeted compute node. Changes to the power-on policy setting take effect after the next restart of the compute node.<br>**Note:** The -ap, -sms, -wol, -local, and -d command options can be entered together, but these options must be used exclusive of all other command options. | `power -ap` *policy*<br>where *policy* is:<br>• `restore` : the compute node will power on if it was previously on<br>• `auto` : when power is applied to the Lenovo Flex System chassis, the compute node will be powered on<br>• `manual` : the compute node will remain off until manually powered on<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade configuration<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |

*Table 60. power command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set restart delay for compute node** | Sets the amount of time that the targeted compute node waits to start after application of power to the Lenovo Flex System chassis. Changes to the restart delay take effect after the next restart of the compute node.<br>**Note:** The -d, -sms, -wol, -local, and -ap command options can be entered together, but these options must be used exclusive of all other command options. | `power -d` *value*<br>where *value* is from 0 to 3600 seconds, inclusive. If you enter a value of 0, the restart delay is disabled (no delay). If you enter a value greater than 3600, an error will be displayed.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade configuration<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |
| **Set restart delay for I/O-module** | Sets the amount of time that the targeted I/O-module waits to start after application of power to the Lenovo Flex System chassis. Changes to the restart delay take effect after the next restart of the I/O-module.<br>**Note:** The -d, -sms, -wol, -local, and -ap command options can be entered together, but these options must be used exclusive of all other command options. | `power -d` *value*<br>where *value* is from 0 to 3600 seconds, inclusive. If you enter a value of 0, the restart delay is disabled (no delay). If you enter a value greater than 3600, an error will be displayed.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• I/O module administration<br>See "Commands and user authority" on page 10 for additional information. | I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |
| **Display POST status for I/O module** | Displays the POST status for the specified I/O module. If the command is run while POST is in progress, it returns the level of POST that is currently in process. If the command is run after POST is complete, it displays one of the following return values:<br>• The `POST results could not be read.` message displays if there was an internal error during POST.<br>• The `POST results not complete: hex_code` message displays if | `power -state -post` | I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |

*Table 60. power command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | POST results are not available after POST completes.<br>• If POST returns valid results, one of the following messages displays:<br>– *hex_code*: `Base internal function failure detected.`<br>– *hex_code*: `Internal interface failure detected.`<br>– *hex_code*: `External interface failure detected.`<br>– *hex_code*: `Module completed POST successfully.`<br>– *hex_code*: `Cannot decode POST result code.`<br>• The `Invalid POST results.` message displays if none of the above conditions is true.<br>Where *hex_code* is a hexadecimal code. See the documentation that comes with your I/O module for information.<br>**Note:** This command option is not supported for serial concentrator I/O modules. | | |

**Example:**

To display the power state for the compute node in compute node bay 5, while this compute node is set as the persistent command environment, at the `system:blade[5]>` prompt, type

```
power -state
```

To turn on the compute node in node bay 5, while this compute node is set as the persistent command environment, at the `system:blade[5]>` prompt, type

```
power -on
```

To display the power state for the compute node in node bay 5 again, while this compute node is set as the persistent command environment, at the `system:blade[5]>` prompt, type

```
power -state
```

The following example shows the information that is returned from these three commands:

```
system:blade[5]> power -state
Off
system:blade[5]> power -on
OK
system:blade[5]> power -state
On
system:blade[5]>
```

## pwrprofile command

This command displays and configures power groups and schedules for compute nodes and I/O modules.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "pwrprofile command errors" on page 453 for a list of error messages that are specific to the pwrprofile command.

*Table 61. pwrprofile command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display all power groups and schedules** | Displays all power groups and schedules configured for the Lenovo Flex System chassis. | `pwrprofile` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Display power group** | Displays information for the specified power group. | `pwrprofile -`*group_index*<br>where *group_index* is the index number that identifies the power group. Index numbers are assigned automatically at group creation and can be seen in the "Display all power groups and schedules" list. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 61. pwrprofile command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Add power group** | Adds a power group with the specified name for the specified key group of compute nodes and I/O modules.<br>**Notes:**<br>• All parameters must be specified when creating a power group.<br>• The index number for the power group is assigned automatically and can be seen in the "Display all power groups and schedules" list. | `pwrprofile -add -n` *name* `-key` *group_key* `-servers` *server_group*<br>where:<br>• *name* is a alphanumeric string up to 63 characters in length that can include periods ( . ) and underscores ( _ ). Each of the 32 group names must be unique.<br>• *group_key* is:<br>– `tm` for type/model<br>– `sn` for serial number<br>– `by` for bay number<br>• *server_group* is:<br>– Type/model or serial number (maximum 31 characters). The wildcard character (*) is accepted.<br>– Bay designations that meet the following criteria:<br>– Maximum string length of 127 characters.<br>– One or more bay-type keywords (`blade` and `switch` are the only keywords supported at this time), each followed by a comma delimited list of bay numbers or range of bay numbers (two bay numbers separated by a dash) surrounded by parentheses.<br>– Bay-type keywords can be in any order separated by a comma.<br>*(continued on next page)* | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Add power group** *(continued)* | | • *server_group (continued)*:<br>– Bay designations *(continued)*: | |

Table 61. pwrprofile command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | | – Individual bay numbers and ranges can be in any order. Overlapping ranges and whitespace are allowed.<br>For example:<br>– blade (1, 3, 4-6, 8, 2-5, 12, 13-14)<br>– blade (3), blade (5-9, 2)<br>– switch (1-2) ,blade (1), switch (4)<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>• Chassis log management<br>• Chassis administration<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | |
| **Add power schedule and assign to power group** | Adds a power schedule, assigned to a specific power group, with the specified name for the specified key group of compute nodes or I/O modules.<br>**Important:** The power group index must be the first command option specified (for example, `pwrprofile -1 -add -s enabled -a on -f once -d 11202015` ).<br>**Notes:**<br>• The power group index, -s, -a, and -f parameters must be specified when creating a power schedule.<br>• If the frequency (-f) is set to once, you must specify either a time (-t), a date (-d), or both a time and date. If only a date is specified, the scheduled action will take place when the system switches to the date indicated.<br>• If the frequency (-f) is set to daily, you must specify a time (-t). | `pwrprofile -`*group_index* `-add -s` *status* `-a` *action* `-f` *freq* `-d` *day* `-t` *time*<br>where:<br>• where *group_index* is the index number that identifies the power group where this schedule will be applied. Index numbers are assigned automatically at group creation and can be seen in the "Display all power groups and schedules" list.<br>• *status* is a power schedule status of `enabled` or `disabled`.<br>• *action* is the power action to perform: `on`, `off`, `cycle`, or `softoff`.<br>• *freq* is how often the schedule is applied: `once`, `daily`, or `weekly`. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 61. pwrprofile command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | - If the frequency (-f) is set to weekly, you must specify both a time (-t) and a day (-d).<br>- Up to four power schedules can be assigned to a power group.<br>- The index number for the power schedule is assigned automatically and can be seen in the "Display all power groups and schedules" list. | - *day* is:<br>  – For frequency of once, a date in `mmddyyyy` format.<br>  – For weekly frequency: `mon`, `tues`, `wed`, `thur`, `fri`, `sat`, or `sun`.<br>- *time* is the time of day in `hhmm` format.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>- Supervisor<br>- Chassis account management<br>- Chassis log management<br>- Chassis administration<br>- Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | |
| **Modify power group** | Changes values for the specified power group.<br>**Important:** The power group index must be the first command option specified (for example, `pwrprofile -1 -n group2` ).<br><br>**Note:** You can modify any valid subset of values for the power group. | `pwrprofile -`*group_index* `-n` *name* `-key` *group_key* `-servers` *server_group*<br>where:<br>- where *group_index* is the index number that identifies the power group to modify. Index numbers are assigned automatically at group creation and can be seen in the "Display all power groups and schedules" list.<br>- *name* is a alphanumeric string up to 63 characters in length that can include periods ( . ) and underscores ( _ ). Each of the 32 group names must be unique.<br>- *group_key* is:<br>  – `tm` for type/model<br>  – `sn` for serial number<br>  – `by` for bay number<br>- *server_group* is:<br>  – Type/model or serial number (maximum | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 61. pwrprofile command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | | 31 characters). The wildcard character (*) is accepted.<br>– Bay designations that meet the following criteria:<br>– Maximum string length of 127 characters.<br>– One or more bay-type keywords (`blade` and `switch` are the only keywords supported at this time), each followed by a comma delimited list of bay numbers or range of bay numbers (two bay numbers separated by a dash) surrounded by parentheses.<br>– Bay-type keywords can be in any order separated by a comma.<br>– Individual bay numbers and ranges can be in any order. Overlapping ranges and whitespace are allowed.<br>For example:<br>• blade (1, 3, 4-6, 8, 2-5, 12, 13-14)<br>• blade (3), blade (5-9, 2)<br>• switch (1-2), blade (1), switch (4)<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management | |

Table 61. pwrprofile command (continued)

| Function | What it does | Command | Target (see paths in "Command targets" on page 6) |
|---|---|---|---|
| | | • Chassis log management<br>• Chassis administration<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | |
| **Modify power schedule** | Changes values for the specified power schedule.<br>**Notes:**<br>• You can modify any valid subset of values for the power schedule.<br>• If the frequency (-f) is set to once, you must specify either a time (-t), a date (-d), or both a time and date. If only a date is specified, the scheduled action will take place when the system switches to the date indicated.<br>• If the frequency (-f) is set to daily, you must specify a time (-t).<br>• If the frequency (-f) is set to weekly, you must specify both a time (-t) and a day (-d). | `pwrprofile -i` *index* `-s` *status* `-a` *action* `-f` *freq* `-d` *day* `-t` *time*<br>where:<br>• where *index* is the index number that identifies the power schedule to modify. Index numbers are assigned automatically at schedule creation and can be seen in the "Display all power groups and schedules" list.<br>• *status* is a power schedule status of `enabled` or `disabled`.<br>• *action* is the power action to perform: `on`, `off`, `cycle`, or `softoff`.<br>• *freq* is how often the schedule is applied: `once`, `daily`, or `weekly`.<br>• *day* is:<br>– For frequency of once, a date in `mmddyyyy` format.<br>– For weekly frequency: `mon`, `tues`, `wed`, `thur`, `fri`, `sat`, or `sun`.<br>• *time* is the time of day in `hhmm` format.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>• Chassis log management<br>• Chassis administration<br>• Chassis configuration<br>See "Commands and user | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 61. pwrprofile command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | | authority" on page 10 for additional information. | |
| **Delete power group** | Deletes the specified power group.<br>**Important:** The power group index must be the first command option specified (for example, `pwrprofile -1 -clear`). | `pwrprofile -`*group_index* `-clear`<br>where *group_index* is the index number that identifies the power group. Index numbers are assigned automatically at group creation and can be seen in the "Display all power groups and schedules" list.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>• Chassis log management<br>• Chassis administration<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 61. pwrprofile command (continued)*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Delete power schedule** | Deletes the specified power schedule. | `pwrprofile -clear -i` *index*<br>where *index* is the index number that identifies the power schedule. Index numbers are assigned automatically at schedule creation and can be seen in the "Display all power groups and schedules" list.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>• Chassis log management<br>• Chassis administration<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

**Example:**

To display information for all power profiles, while the primary CMM in bay 2 is set as the persistent command environment, at the `system:mm[2]>` prompt, type

```
pwrprofile
```

To add a power profile named g1 that is keyed by bay number and includes the compute nodes in node bays 1 and 2, and the I/O module in I/O-module bay 3, while the primary CMM in bay 2 is set as the persistent command environment, at the `system:mm[2]>` prompt, type

```
pwrprofile -add -n g1 -key by -servers blade(1,2),switch(3)
```

To add a power schedule to power group g1 (index 1) and enable this new power schedule that turns on the compute nodes in power group 1 once on 11 November 2015 at 11:11 AM, while the primary CMM in bay 2 is set as the persistent command environment, at the `system:mm[2]>` prompt, type

```
pwrprofile -1 -add -s enabled -a on -f once -d 11202015 -t 1111
```

To delete power schedule 1, while the primary CMM in bay 2 is set as the persistent command environment, at the `system:mm[2]>` prompt, type

```
pwrprofile -i 1 -clear
```

The following example shows the information that is returned from these commands:

```
system:mm[2]> pwrprofile
No group found
system:mm[2]>  pwrprofile -add -n g1 -key by -servers blade(1,2),switch(3)
Group 1 added
```

```
system:mm[2]>  pwrprofile

1. g1
   key: by
   servers: blade(1,2),switch(3)
   power schedules: Not Available

system:mm[2]>  pwrprofile -1 -add -s enabled -a on -f once -d 11202015 -t 1111
Power schedule 1 added
system:mm[2]>  pwrprofile

1. g1
   key: by
   servers: blade(1,2),switch(3)
   power schedules:

        -i 1
        -s enabled
        -a on
        -f once
        -d 11/20/2015
        -t 1111

system:mm[2]>  pwrprofile -i 1 -clear
OK
system:mm[2]>  pwrprofile

1. g1
   key: by
   servers: blade(1,2),switch(3)
   power schedules: Not Available

system:mm[2]>  pwrprofile -1 -clear
OK
system:mm[2]>  pwrprofile
No group found
system:mm[2]>
```

## read command

This command restores the CMM configuration, including users and permission groups, that was previously saved to a file. It can also be used to unmanage the CMM after a failed or incomplete unmanage operation.

Configurations are saved to a file using the “write command” on page 404.

**Notes:**

- To successfully restore all settings using the `read` command, a user must have permission to modify any settings controlled by individual commands in the configuration being restored.
- Restoring the CMM overwrites all existing user accounts and passwords on the CMM and the CMM IP address with the values in the backup file.
- When a CMM is managed by an external management device, user management for CMM accounts is performed by that management device. User accounts and certificates on the CMM are locked, and the necessary certificates are not included in the CMM backup image, which will cause communications between the management device and the CMM to fail. See "Re-managing a CMM after restoring its configuration," in the *Lenovo Chassis Management Module 2 Installation Guide*, for information about re-managing a restored CMM.

- When the CMM is set to “Secure” security mode, only secure file transfer methods, such as HTTPS and SFTP, can be used for tasks involving file transfer when the CMM is acting as a server. Unsecure file transfer protocols, such as HTTP, FTP, and TFTP, are disabled when the CMM is acting as a server when the security mode is set to “Secure”. Unsecure file transfer protocols remain available for a CMM acting as a client for all commands when the security mode is set to “Secure”.
- For information about how to specify a URL for file transfer, see “Specifying a URL for file transfer” on page 29.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See “Common errors” on page 407 for a list of error messages that apply to all commands or “read command errors” on page 456 for a list of error messages that are specific to the read command.

Table 62. read command

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Restore CMM configuration from file** | Restores the CMM configuration from an image that was previously saved to a file.<br>**Notes:**<br>- This image includes CMM users and permission groups.<br>- Password information stored in the configuration file is encrypted.<br>- Users must have permission to modify any settings controlled by individual commands in the configuration being restored. | `read -u` *URL* `-p` *passphrase*<br>where:<br>- *URL* is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the configuration file is located.<br>- "*passphrase*" is the double-quote delimited passphrase that was used to save the original configuration file. Minimum passphrase length is 6 characters. Maximum passphrase length is 31 characters.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>- Supervisor<br>- Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Restore CMM configuration from file (verbose)** | Restores the CMM configuration from an image that was previously saved to a file, showing the log file generated while doing the restore. The log file is not shown until the restore is complete, which might take several minutes.<br>**Notes:**<br>- This image includes CMM users and permission groups.<br>- Password information stored in the configuration file is encrypted.<br>- Users must have permission to modify any settings controlled by individual commands in the configuration being restored. | `read -u` *URL* `-p` *passphrase* `-v`<br>where:<br>- *URL* is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the configuration file is located.<br>- "*passphrase*" is the double-quote delimited passphrase that was used to save the original configuration file. Minimum passphrase length is 6 characters. Maximum passphrase length is 31 characters. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 62. read command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | | This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | |
| **Restore CMM configuration from file and reset CMM** | Restores the CMM configuration from an image that was previously saved to a file and then reset the CMM.<br>**Notes:**<br>• This image includes CMM users and permission groups.<br>• Password information stored in the configuration file is encrypted.<br>• The CMM resets in all cases, even if restoring the configuration fails.<br>• Users must have permission to modify any settings controlled by individual commands in the configuration being restored. | `read -u` *URL* `-p` *passphrase* `-r`<br>where:<br>• *URL* is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the configuration file is located.<br>• "*passphrase*" is the double-quote delimited passphrase that was used to save the original configuration file. Minimum passphrase length is 6 characters. Maximum passphrase length is 31 characters.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 62. read command (continued)*

| Function | What it does | Command | **Target** *(see paths in "*Command targets*" on page 6)* |
|---|---|---|---|
| **Restore CMM configuration from file (verbose) and reset CMM** | Restores the CMM configuration from an image that was previously saved to a file, showing the log file generated while doing the restore. The log file is not shown until the restore is complete, which might take several minutes, and displays for several seconds until the CMM resets.<br>**Notes:**<br>• This image includes CMM users and permission groups.<br>• Password information stored in the configuration file is encrypted.<br>• The CMM resets in all cases, even if restoring the configuration fails.<br>• Users must have permission to modify any settings controlled by individual commands in the configuration being restored. | `read -u` *URL* `-p` *passphrase* `-v -r`<br>where:<br>• *URL* is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the configuration file is located.<br>• "*passphrase*" is the double-quote delimited passphrase that was used to save the original configuration file. Minimum passphrase length is 6 characters. Maximum passphrase length is 31 characters.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Unmanage CMM (forced)** | Unmanages the CMM after a failed or incomplete unmanage operation. | `read -f unmanage`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

**Example:**

To restore the CMM configuration from an image previously saved to a file named cmm1.cfg in the temp directory on a TFTP server with an IP address of 9.37.177.215 and a passphrase of backuplock, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
read -u tftp://9.37.177.215/temp/cmm1.cfg -p "backuplock" -T mm[p]
```

The following example shows the information that is returned from this command:

```
system> read -u tftp://9.37.177.215/temp/cmm1.cfg -p "backuplock" -T mm[p]
OK
Configuration restore was successful
Restart the MM for the new settings to take effect
system>
```

To restore the CMM configuration from an image previously saved to a file named cfg.bkp in the /tftpboot/ backup directory on a SFTP server with an IP address of 300.370.640.310, a user ID of userid, and a passphrase of Passphaase, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
read -u sftp://userid:password@300.370.640.310/tftpboot/backup/cfg.bkp
-p "Passphaase" -T mm[p]
```

The following example shows the information that is returned from this command:

```
system> read -u sftp://userid:password@300.370.640.310/tftpboot/backup/cfg.bkp
-p "Passphaase" -T mm[p]
OK
Configuration restore was successful
Restart the MM for the new settings to take effect
system>
```

## remotechassis command

This command displays and manages the list of each Lenovo Flex System chassis that the CMM discovers on the network.

**Note:** The CMM that runs the remotechassis command is also included in all lists.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "remotechassis command errors" on page 457 for a list of error messages that are specific to the remotechassis command.

*Table 63. remotechassis command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display complete list** | Displays a list of all Lenovo Flex System chassis that the CMM discovers on the network. The list includes the following information about each Lenovo Flex System chassis:<br>• Name<br>• IP address<br>• Status<br>• Firmware level<br>• Type<br>• Serial number<br>• FRU number<br>• Chassis serial number<br>• Chassis FRU number<br>• Chassis machine-type model (MTM)<br>• Chassis UUID | `remotechassis` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Display list grouped by health status** | Displays a list of names for Lenovo Flex System chassis that the CMM discovers on the network. The list is grouped by health status. | `remotechassis -health` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Display list filtered by IP address** | Displays a list of Lenovo Flex System chassis that the CMM discovers on the network, filtered by the specified IP address. The list includes the following information about each Lenovo Flex System chassis:<br>• Name<br>• IP address<br>• Status<br>• Firmware level<br>• Type<br>• Serial number<br>• FRU number<br>• Chassis serial number<br>• Chassis FRU number<br>• Chassis machine-type model (MTM)<br>• Chassis UUID | `remotechassis -ip` *ip_address*<br>where *ip_address* is an IP address pattern that uses the asterisk (*) as a wildcard (for example; 201.47.123.*). | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 63. remotechassis command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display list filtered by name** | Displays a list of Lenovo Flex System chassis that the CMM discovers on the network, filtered by the specified name. The list includes the following information about each Lenovo Flex System chassis:<br>• Name<br>• IP address<br>• Status<br>• Firmware level<br>• Type<br>• Serial number<br>• FRU number<br>• Chassis serial number<br>• Chassis FRU number<br>• Chassis machine-type model (MTM)<br>• Chassis UUID | `remotechassis -name` *name*<br>where *name* is a name pattern that uses the asterisk (*) as a wildcard (for example; WebServer*). | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Clear list** | Clears the list of Lenovo Flex System chassis that the CMM discovered on the network. | `remotechassis -clear` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

### Example:

To list all Lenovo Flex System chassis on the network with a name starting with "WebServer", while the primary CMM in bay 1, that does not support IPv6, is set as the persistent command environment, at the `system:mm[1]>` prompt, type

`remotechassis -name WebServer*`

The following example shows the information that is returned from this command:

```
system:mm[1]> remotechassis -name WebServer*
Running chassis discovery...
-----------------------------------------------------
Name:             WebServer001
IP:              145.48.204.212
Status:          normal
Firmware:       BPET25L,CNETMNUS.PKT,01-08-07,37,1
Type:            CMM
Serial:        0J1M9E585630
FRU:             25R5777
Chassis Serial: 23A2343
Chassis FRU:     25R5780R5780
Chassis MTM:     885222Z
Chassis UUID:    4E349451FA8011D9B10C89E0183AD13D
-----------------------------------------------------
Name:             WebServer002
IP:              145.48.204.222
```

```
Status:          normal
Firmware:        BPET25L,CNETMNUS.PKT,01-08-07,37,1
Type:            CMM
Serial:          0J1M9E585656
FRU:             25R5777
Chassis Serial: 23A2356
Chassis FRU:     25R5780R5780
Chassis MTM:     885222Z
Chassis UUID:    4E325951FA8011D9B86C89E0183AD02D
------------------------------------------------------
system:mm[1]>
```

To list all Lenovo Flex System chassis on the network with a name starting with "SYSTEM*", while the primary CMM in bay 1, that supports IPv6, is set as the persistent command environment, at the `system:mm[1]>` prompt, type
`remotechassis -name SYSTEM*`

The following example shows the information that is returned from this command:

```
system:mm[1]> remotechassis -name SYSTEM*
Running chassis discovery...
------------------------------------------------------
Name:             SYSTEM
IP:              10.13.1.190
IPv6:            2002:1013::211:25ff:fec3:227c
                  2001:1013::211:25ff:fec3:227c
                  2000:1013::211:25ff:fec3:227c
                  fe80::211:25ff:fec3:227c
                  2000:1013::a1be:a348:7672:2def
                  2000:1013::1:191
Status:          critical
Firmware:        BPET002,CNETMNUS.PKT,02-17-10,1
Type:            CMM
Serial:          YK118165A117
FRU:             39Y9661
Chassis Serial: KQWPLB9
Chassis FRU:     44X2302
Chassis MTM:     8852HC1
Chassis UUID:    E13112E1829448E29999DA2066681D89
------------------------------------------------------
Name:             SYSTEM
IP:              10.13.1.30
IPv6:            2000:1013::fc58:325c:c8b4:9c4c
                  2000:1013::214:5eff:fed0:2e1c
                  2000:1013::1:30
                  fe80::5652:ff:fe69:d763
                  2002:1013::211:25ff:fec3:8cfa
                  2001:1013::211:25ff:fec3:8cfa
                  2000:1013::211:25ff:fec3:8cfa
                  fe80::211:25ff:fec3:8cfa
Status:          attention
Firmware:        BPET54A,CNETMNUS.PKT,02-17-10,84
Type:            CMM-telco
Serial:          YK118269Y115
FRU:             39Y9661
Chassis Serial: 23A0052
Chassis FRU:     42C3673
Chassis MTM:     87501RZ
Chassis UUID:    B5BAEC01A10B11DB9F3BC1BE8FFF3B3C
------------------------------------------------------
```

```
system:mm[1]>
```

## reset command

This command resets compute nodes, compute node system-management processors, I/O modules, or the primary CMM. It also resets the multiplexer expansion module.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "reset command errors" on page 457 for a list of error messages that are specific to the reset command.

*Table 64. reset command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Reset** | Performs an immediate reset and restart of the specified device. | `reset`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade administration (for compute node or compute node ISMP)<br>• I/O module administration (for I/O module)<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number.<br>Compute node system-management processor:<br>`sp`<br>I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |
| **Reset primary CMM** | Performs an immediate reset and restart of the primary CMM. If the current operating state of the Lenovo Flex System chassis indicates potential problems with performing the reset, an error message is returned and the reset is cancelled. | `reset`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis administration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Reset primary CMM (with override)** | Performs an immediate reset and restart of the primary CMM, overriding error messages and reset cancellation due to the current Lenovo Flex System chassis operating state. | `reset -o`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis administration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 64. reset command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Reset standby CMM** | Performs an immediate reset of the standby CMM. | `reset -standby`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis administration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number.<br>**Note:** Even though this command resets the standby CMM, it still must specify the primary CMM as the command target. |
| **Reset compute node to command console** | Opens a command console with an SOL session when the specified compute node is reset. | `reset -c`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade administration and blade remote presence<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |
| **Reset with failover** | Resets the specified command target, enabling failover if a redundant (standby) component for the command target is present.<br>An error message is displayed if you try to failover from the primary CMM when a standby CMM is not installed or if the firmware in the one of the CMMs is updating. | `reset -f`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis administration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Reset I/O module with standard diagnostics** | Performs an immediate reset and restart of the specified device, running standard diagnostics on the I/O module after it restarts.<br>Running the `reset -std` command gives the same result as running the `reset` command on a I/O module. | `reset -std`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• I/O module administration<br>See "Commands and user authority" on page 10 for additional information. | I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |

*Table 64. reset command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Reset I/O module with extended diagnostics** | Performs an immediate reset and restart of the specified device, running extended diagnostics on the I/O module after it restarts. | `reset -exd`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• I/O module administration<br>See "Commands and user authority" on page 10 for additional information. | I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |
| **Reset I/O module with full diagnostics** | Performs an immediate reset and restart of the specified device, running full diagnostics on the I/O module after it restarts. | `reset -full`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• I/O module administration<br>See "Commands and user authority" on page 10 for additional information. | I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |
| **Restart compute node with NMI** | Performs an immediate reset and restart of the specified compute node, for compute nodes that support the non-maskable interrupt (NMI).<br>**Note:** A compute node must be powered on to run the `reset -sft` command. | `reset -sft`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade administration and blade remote presence<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |

**Example:** To reset the system-management processor on the compute node in node bay 5, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type `reset -T blade[5]:sp`

The following example shows the information that is returned:

```
system> reset -T blade[5]:sp
OK
system>
```

## scale command

This command displays the partition control and configuration settings for multiple compute nodes or nodes in a scalable complex, for compute nodes installed in the Lenovo Flex System chassis that support this feature.

**Notes:**

- The scale command will execute only on compute nodes that support scalable complexes.
- All compute nodes in a scalable complex must be at the same firmware level. When scripting firmware updates for compute nodes in a scalable complex, make sure that the `update` commands are included for each node in the complex.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "scale command errors" on page 459 for a list of error messages that are specific to the scale command.

*Table 65. scale command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display all scalable complex information** | Displays all scalable complex information for the Lenovo Flex System chassis. | `scale` | Lenovo Flex System chassis:<br>`system` |
| **Display information for specific scalable complex** | Displays information for the specified scalable complex.<br>**Notes:**<br>• The *complex_id* is found by running the `scale` command with no options.<br>• The `-compid` command option is required for only compute node systems that can have multiple scalable complexes defined in the same Lenovo Flex System chassis. This option does not need to be specified for stand-alone systems. | `scale -compid` *complex_id* where *complex_id* is a unique complex identifier (hexadecimal string of four alphanumeric characters), assigned by the compute node complex. | Lenovo Flex System chassis:<br>`system` |

*Table 65. scale command (continued)*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display information for specific node in a scalable complex** | Displays information for a specific node in the scalable complex.<br>**Notes:**<br>• The *complex_id* and *node_id* are found by running the `scale` command with no options.<br>• The `-compid` command option is required for only compute node systems that can have multiple scalable complexes defined in the same Lenovo Flex System chassis. This option does not need to be specified for stand-alone systems. | `scale -compid` *complex_id* `-node` *node_id*<br>where :<br>• *complex_id* is a unique complex identifier (hexadecimal string of four alphanumeric characters), assigned by the compute node complex.<br>• *node_id* is the compute node bay number, of the node. | Lenovo Flex System chassis:<br>`system` |
| **Display information for specific partition in a scalable complex** | Displays information for a specific partition in the scalable complex.<br>**Notes:**<br>• The *complex_id* and *partition_id* are found by running the `scale` command with no options.<br>• The `-compid` command option is required for only compute node systems that can have multiple scalable complexes defined in the same Lenovo Flex System chassis. This option does not need to be specified for stand-alone systems. | `scale -compid` *complex_id* `-partid` *partition_id*<br>where :<br>• *complex_id* is a unique complex identifier (hexadecimal string of four alphanumeric characters), assigned by the compute node complex.<br>• *partition_id* is a partition identifier, assigned by the compute node complex. | Lenovo Flex System chassis:<br>`system` |

**Example:** To view all scalable complexes in the system, while the Lenovo Flex System chassis is set as the persistent command environment, at the system> prompt, type

```
scale
```

To view information about the scalable complex with an ID of D787, while the Lenovo Flex System chassis is set as the persistent command environment, at the system> prompt, type

```
scale -compid D787
```

To view information about the partition with an ID of 1 in the scalable complex with an ID of D787, while the Lenovo Flex System chassis is set as the persistent command environment, at the system> prompt, type

```
scale -compid D787 -partid 1
```

To view information about the compute node with an ID of 7 in the scalable complex with an ID of D787, while the Lenovo Flex System chassis is set as the persistent command environment, at the system> prompt, type

```
scale -compid D787 -node 7
```

The following example shows the information that is returned from these commands:

```
system> scale

--- Complex ID: D787 ---
```

```
Partition ID: 1
Assigned Nodes:
---------------

        Bay: 1
        Name: Node 01
        Processors/Memory: 2 Intel Xeon/2 DIMMs 4GB
        Logical Node ID: 0
        Status: powered off
        Mode: partition
        Primary: Yes

        Bay: 3
        Name: Node 03
        Processors/Memory: 2 Intel Xeon/2 DIMMs 4GB
        Logical Node ID: 1
        Status: powered on
        Mode: partition
        Primary: No

        Bay: 5
        Name: Node 05
        Processors/Memory: 2 Intel Xeon/2 DIMMs 4GB
        Logical Node ID: 2
        Status: powered off
        Mode: partition
        Primary: No

        Bay: 7
        Name: Node 07
        Processors/Memory: 2 Intel Xeon/2 DIMMs 4GB
        Logical Node ID: 3
        Status: powered off
        Mode: partition
        Primary: No

system> scale -compid D787

Partition ID: 1
Assigned Nodes:
---------------

        Bay: 1
        Name: Node 01
        Processors/Memory: 2 Intel Xeon/2 DIMMs 4GB
        Logical Node ID: 0
        Status: powered off
        Mode: partition
        Primary: Yes

        Bay: 3
        Name: Node 03
        Processors/Memory: 2 Intel Xeon/2 DIMMs 4GB
        Logical Node ID: 1
        Status: powered on
        Mode: partition
        Primary: No

        Bay: 5
        Name: Node 05
        Processors/Memory: 2 Intel Xeon/2 DIMMs 4GB
        Logical Node ID: 2
        Status: powered off
        Mode: partition
        Primary: No

        Bay: 7
        Name: Node 07
        Processors/Memory: 2 Intel Xeon/2 DIMMs 4GB
        Logical Node ID: 3
        Status: powered off
        Mode: partition
        Primary: No

system> scale -compid D787 -partid 1

Partition ID: 1
Assigned Nodes:
---------------

        Bay: 1
        Name: Node 01
        Processors/Memory: 2 Intel Xeon/2 DIMMs 4GB
        Logical Node ID: 0
        Status: powered off
        Mode: partition
        Primary: Yes

        Bay: 3
        Name: Node 03
        Processors/Memory: 2 Intel Xeon/2 DIMMs 4GB
        Logical Node ID: 1
        Status: powered on
        Mode: partition
        Primary: No

        Bay: 5
        Name: Node 05
        Processors/Memory: 2 Intel Xeon/2 DIMMs 4GB
        Logical Node ID: 2
        Status: powered off
        Mode: partition
        Primary: No

        Bay: 7
        Name: Node 07
        Processors/Memory: 2 Intel Xeon/2 DIMMs 4GB
        Logical Node ID: 3
        Status: powered off
        Mode: partition
        Primary: No

system> scale -compid D787 -node 7

UUID: 0C5513A7 25274D0B 931EDEC6 95571364
Serial Number: NANWOOR
Checksum: 3403
Number of Ports: 3
Ports:
------
```

```
        Port ID: 0
        Remote Checksum: A100
        Remote Port ID: 2
        Status: Enabled
        Type: QPI

        Port ID: 1
        Remote Checksum: D401
        Remote Port ID: 2
        Status: Enabled
        Type: QPI

        Port ID: 2
        Remote Checksum: 7402
        Remote Port ID: 2
        Status: Enabled
        Type: QPI

system>
```

## sddump command

This command initiates a dump of service data from compute nodes, and I/O modules that support this function.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "sddump command errors" on page 459 for a list of error messages that are specific to the sddump command.

*Table 66. sddump command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Dump service data (compute node)** | Dumps service data of the specified type from the specified compute node target.<br>• For compute nodes with an IMM, data dumps are initiated and collected from the CMM.<br>• For compute nodes that do not have an IMM, data dumps can be initiated, but are not collected, from the CMM; these data dumps remain on the compute node. | `sddump -init`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade administration<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[x]`<br>where *x* is the node bay number. |
| **Dump service data (I/O module)** | Dumps service data from the specified I/O-module target.<br>**Note:** To successfully obtain a data dump from an I/O module, the I/O module must support data collection. | `sddump -init` | I/O module:<br>`switch[x]`<br>where *x* is the I/O-bay number. |
| **Get service data** | Collects service data, from the last generated service-data dump, of the specified type from the specified compute node target. | `sddump -coll`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade administration<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[x]`<br>where *x* is the node bay number. |

**Example:** To initiate a data dump from the system-management processor of the compute node in bay 2, while this compute node is set as the persistent command environment, at the `system:blade[2]>` prompt, type `sddump -init`

The following example shows the information that is returned from this command:

```
system:blade[2]> sddump -init
OK
system:blade[2]>
```

## sdemail command

This command sends an email with the service information to the specified recipients.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "sdemail command errors" on page 460 for a list of error messages that are specific to the sdemail command.

Table 67. sdemail command

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Send service information using email to specified recipients** | Send an email with service information to the specified recipients. You assign a subject and an email address. When you run this command, it attaches the service log to the message. | `sdemail -subj` "*subject*"`-to` *address*<br>where:<br>- "*subject*" is a quote-delimited text string up to 119 characters in length.<br>- *address* is the recipients email address. Multiple addresses separated with a comma can be entered (119 characters maximum).<br><br>This command can only be run by users who have one or more of the following command authorities:<br>- Supervisor<br>- Chassis account management<br>- Chassis log management<br>- Chassis administration<br>- Chassis configuration<br>- Blade administration<br>- Blade configuration<br>- Blade remote presence<br>- I/O module administration<br>- I/O module configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

**Example:**

To send a service information email message, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type
`sdemail -T mm[p] -to mail@lenovo.com -subj "Blade 8 Reboot"`

The following example shows the information that is returned from this command:

```
system> sdemail -T mm[p] -to mail@lenovo.com -subj "Blade 8 Reboot"
OK
system>
```

## security command

This command sets and displays the chassis security policy level for the CMM.

**Notes:**

- You cannot access the CMM CLI through Telnet while using the Secure chassis security policy setting.
- When the CMM is set to “Secure” security mode, only secure file transfer methods, such as HTTPS and SFTP, can be used for tasks involving file transfer when the CMM is acting as a server. Unsecure file transfer protocols, such as HTTP, FTP, and TFTP, are disabled when the CMM is acting as a server when the security mode is set to “Secure”. Unsecure file transfer protocols remain available for a CMM acting as a client for all commands when the security mode is set to “Secure”.
- The CMM HTTP and HTTPS ports are open at all times. Port behavior is determined by the CMM HTTPS port setting, which can be affected by the CMM chassis security policy setting:
  - When the CMM HTTPS port is enabled, the HTTP port (port 80) remains open and redirects to the HTTPS port (port 443). When the chassis security policy is set to secure, the CMM HTTPS port is automatically enabled and its setting cannot be changed.
  - When the CMM HTTPS port is disabled, the HTTPS port (port 443) remains open and redirects to the HTTP port (port 80).

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See “Common errors” on page 407 for a list of error messages that apply to all commands or “security command errors” on page 460 for a list of error messages that are specific to the security command.

Table 68. security command

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display CMM chassis security policy** | Displays the chassis security policy information for the CMM:<br>• Security policy level (legacy or secure).<br>• Security policy state:<br>– Active indicates that the security policy is in force.<br>– Pending indicates that the changes are needed, such as disabling non-secure protocols, before the policy can become active.<br>• Version of the security policy rule definitions being enforced. | `security` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set CMM chassis security policy level** | Sets the chassis security policy level for the CMM.<br>**Notes:**<br>• To set the chassis security policy level to secure, "accseccfg command" on page 39 options must be set as follows:<br>– -cp (complex password): on<br>– -de (default account password change at next login): on<br>– -pc (password change on first access): on<br>• The following interfaces must be disabled, using the "ports command" on page 250, before setting the CMM chassis security level to secure:<br>– HTTP<br>– FTP<br>– SNMPv1<br>– Telnet<br>– TFTP<br>– Non-secure TCP command mode | `security -p` *level*<br>where *level* is `legacy` or `secure` .<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

**Example:**

To display the chassis security policy level setting for the CMM, while the primary CMM in bay 2 is set as the persistent command environment, at the `system:mm[2]>` prompt, type
`security`

The following example shows the information that is returned from this command:

```
system:mm[2]> security
-p legacy
State: active
Version: 01.00
```

```
system:mm[2]>
```

## service command

This command resets a compute node, compute node system-management processor, I/O module, or the primary or standby CMM.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "service command errors" on page 461 for a list of error messages that are specific to the service command.

**Attention:** If you are managing your Lenovo Flex System chassis using a management device, such as the optional Lenovo XClarity Administrator or Flex System Manager software, you must unmanage and remanage the chassis when performing virtual reseat (service-level reset) of the primary CMM using the `service -vr` command. See http://flexsystem.lenovofiles.com/help/topic/com.lenovo.lxca.doc/aug_product_page.html for information about unmanaging and remanaging the chassis using the Lenovo XClarity Administrator application. See http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.8731.doc/product_page.html for information about unmanaging and remanaging the chassis using the Flex System Manager software.

*Table 69. service command*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Virtual reseat** | Performs a virtual reseat (service-level reset) of the specified command target.<br>A virtual reseat simulates physical removal and insertion of the command target. The virtual reseat removes standby power from the command target and then restores it. Each command target type has unique behavior when virtually reseated:<br>• A CMM or I/O module is automatically powered on after the virtual reseat.<br>• A compute node or storage node remains off after a virtual reseat and the user will need to power it back on. The command forcibly shuts down the compute node operating system.<br>• If the -vr command option is run on the primary CMM without specifying the -o command option, warnings about the standby CMM state are displayed.<br>**Attention:**<br>• Performing a virtual reseat on Lenovo Flex System components might result in the loss of data. Do not perform a virtual reseat unless you are instructed by Lenovo Support. Prior to executing a virtual reseat, perform any needed operations to protect user data.<br>• Performing a virtual reseat on a Flex System V7000 storage node (or storage cluster) might result in the loss of data. Do not perform a virtual reseat on a Flex System V7000 storage node (or storage cluster) unless you are instructed by Lenovo Support. Prior to executing a virtual reseat, perform any needed operations to protect user data.<br><br>**Important:**<br>• Instead of performing a virtual reseat on a Flex System V7000 storage node, use the "Powering on and powering off the clustered system" procedure to power off a Flex System V7000 storage node, if needed (see "Powering on and powering off the clustered system" in the Flex System V7000 Storage Node library).<br><br>*(continued on next page)* | `service -vr`<br>This command can only be run by users who have one or more of the following command authorities:<br>• For the CMM target:<br>– Supervisor<br>– Chassis Administration<br>– Chassis Configuration<br>• For the compute node or storage node target:<br>– Supervisor<br>– Blade Administration<br>– Blade Configuration<br>• For the I/O Module target:<br>– Supervisor<br>– I/O Module Administration<br>See "Commands and user authority" on page 10 for additional information. | Primary or standby CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[s]`<br>`mm[S]`<br>`mm[`*x*`]`<br>where *x* is the primary or standby CMM bay number.<br><br>Compute node or storage node:<br>`blade[`*x*`]`<br>where *x* is the node bay number.<br><br>I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |
| **Virtual reseat** *(continued)* | • If you do perform a virtual reseat on a Flex System V7000 storage node, one or more nodes might cause a node error 578 and be unavailable. Use the Flex System V7000 storage node troubleshooting information to troubleshoot issues caused by the virtual reseat option (see "Troubleshooting" in the | | |

*Table 69. service command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
|  | Flex System V7000 Storage Node library).For more information on Flex System V7000 storage node error 578, see "Error 578" in the Flex System V7000 Storage Node library.<br>• During a virtual reseat, the component will experience a temporary loss of communication and its power state will change.<br>• If you are managing your Lenovo Flex System chassis using an optional management device, you must unmanage and remanage the chassis when performing virtual reseat (service-level reset) of the primary CMM. See the documentation for your management device for information.<br>**Note:** Do not perform a virtual reseat on a compute node that indicates it is in maintenance mode. Indications of maintenance mode are shown in the CMM or IMM event logs and by management devices such as the optional Lenovo XClarity Administrator. |  |  |
| **Virtual reseat of primary CMM (suppress warnings for standby CMM)** | Performs a virtual reseat (service-level reset) of the specified command target.<br>A virtual reseat simulates physical removal and insertion of the command target. The virtual reseat removes standby power from the command target and then restores it.<br>• A CMM is automatically powered on after the virtual reseat.<br>• The -o command option suppresses warnings about the standby CMM state.<br>**Attention:**<br>• During a virtual reseat, you will temporarily lose communication with the command target and its power state will change. Before performing a virtual reseat, make sure that you perform any actions necessary to protect user data.<br>• If you are managing your Lenovo Flex System chassis using an optional management device, you must unmanage and remanage the chassis when performing virtual reseat (service-level reset) of the primary CMM. See the documentation for your management device for information. | `service -vr -o`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis Administration<br>• Chassis Configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary or standby CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[s]`<br>`mm[S]`<br>mm[*x*]<br>where *x* is the primary or standby CMM bay number. |

*Table 69. service command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Hard restart** | Performs a hardware reset of the system-management processor of the specified command target. A hard restart directly resets the system-management processor on the command target. The power state of the command target is not affected by this reset.<br>**Notes:**<br>• During a hard restart, you will temporarily lose communication with the command target. Communication between the compute node and its management network should automatically restore after the system-management processor reset is complete.<br>• Not all compute nodes support the hard restart function.<br>• A system-management processor does not need to be responsive in order to reset it. | `service -hard`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Blade Administration<br>• Blade Configuration<br>See "Commands and user authority" on page 10 for additional information. | Compute node system-management processor:<br>`sp` |

**Example:**

The following example shows the information that is returned from these commands:

```
system> service -T switch[1] -vr
OK
system> service -T blade[1]:sp -hard
OK
system>
```

## smtp command

This command configures and displays the CMM SMTP settings.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "smtp command errors" on page 461 for a list of error messages that are specific to the smtp command.

Table 70. smtp command

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display SMTP server host name or IP address** | Displays the SMTP server domain name and host name or IP address. | `smtp` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Server host name or IP address - set** | Checks syntax and sets the server host name or IP address. | `smtp -s` *hostname/ip_address*<br>where *hostname/ip_address* is the host name or IP address of the server. The value can be cleared by setting it to an empty, double-quote delimited string ("").<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **SMTP e-mail server domain name - set** | Checks syntax and sets the SMTP e-mail server domain name. | `smtp -d` *domainname*<br>where *domainname* is a valid domain name that meets the following criteria:<br>• Alphanumeric string up to 63 characters in length.<br>• Can contain dots (.), dashes (-), or underscores (_).<br>• Must contain at least one dot.<br>• No consecutive dots are allowed.<br>• Quotes are not required.<br>• Value can be cleared by setting it to an empty, double-quote delimited string ("").<br>This command can only be run by users who have | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 70. smtp command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
|  |  | one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. |  |

**Example:**

To set the SMTP server host name to lenovo.com, while the primary CMM in bay 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type
`smtp -s lenovo.com`

To display the SMTP configuration, while the primary CMM in bay 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type
`smtp`

The following example shows the information that is returned from these two commands:

```
system:mm[1]> smtp -s lenovo.com
OK
system:mm[1]> smtp
-s lenovo.com
SMTP email domain name is not set
system:mm[1]>
```

## snmp command

This command configures and displays the CMM SNMP settings.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "snmp command errors" on page 462 for a list of error messages that are specific to the snmp command.

*Table 71. snmp command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display SNMP configuration of CMM** | Displays the current SNMP configuration of the CMM. | `snmp` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **SNMPv1 agent - enable/disable** | Enables or disables the CMM SNMPv1 agent.<br>**Notes:**<br>• Before you can enable the SNMPv1 agent, the following must be specified (see "config command" on page 102):<br>– CMM contact name<br>– CMM location<br>– at least one community name<br>– at least one valid IP address for that community<br>• SNMPv1 can not be enabled if the CMM chassis security level is set to secure with the "security command" on page 298. | `snmp -a -`*state*<br>where *state* is `on` or `off` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **SNMPv3 agent - enable/disable** | Enables or disables the CMM SNMPv3 agent.<br>**Notes:** Before you can enable the SNMPv3 agent, the following must be specified:<br>• CMM contact name<br>• CMM location<br>(see "config command" on page 102) | `snmp -a3 -`*state*<br>where *state* is `on` or `off` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **SNMP traps - enable/disable** | Enables or disables the CMM SNMP traps.<br>**Note:** SNMPv1 ports will not be available if the CMM chassis security level is set to secure with the "security command" on page 298. | `snmp -t -`*state*<br>where *state* is `on` or `off` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 71. snmp command (continued)

| Function | What it does | Command | Target *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **SNMP community 1 name - set** | Sets the name of community 1. | `snmp -c1` *name*<br>where *name* is a descriptive name of community 1.<br>• Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments.<br>• If this argument is not specified, the snmp command clears this option.<br>• You can also clear this option by assigning an empty string as its value.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **SNMP community 1 first host name or IP address - set** | Checks syntax and sets the first host name or IP address of community 1. | `snmp -c1i1` *hostname/ip_address*<br>where *hostname/ip_address* is the first host name or IP address of community 1.<br>• The first IP address of the first community can be set to 0.0.0.0 if the community access type is set to GET (for all CMM types) or SET.<br>• Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments.<br>• If this argument is not specified, the snmp command clears this option.<br>• You can also clear this option by assigning an empty string as its value.<br><br>This command can only be run by users who have one | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 71. snmp command (continued)*

| Function | What it does | Command | **Target** *(see paths in* “Command targets” *on page 6)* |
|---|---|---|---|
| | | or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See “Commands and user authority” on page 10 for additional information. | |
| **SNMP Community 1, first host name - set access to SET (wildcard)** | Sets the access type for community 1 to SET. | `snmp –ca1 set -c1i1 0.0.0.0`<br>• With the access type of SET, anyone can query the management information base (MIB) and set MIB values. Using 0.0.0.0 IP address with SET access allows open access to the CMM for write (SET) operations. A 0.0.0.0 address cannot be a trap receiver.<br>• Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments.<br>• If this argument is not specified, the snmp command clears this option.<br>• You can also clear this option by assigning an empty string as its value.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See “Commands and user authority” on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 71. snmp command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **SNMP Community 1, first host name or IP address - set access to GET (wildcard)** | Sets the access type for community 1 to GET. | `snmp -ca1 get -c1i1 0.0.0.0`<br>• With the access type of GET, anyone can query the MIB. Using 0.0.0.0 IP address with GET access allows open access to the CMM for read (GET). A 0.0.0.0 address cannot be a trap receiver.<br>• Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments.<br>• If this argument is not specified, the snmp command clears this option.<br>• You can also clear this option by assigning an empty string as its value.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **SNMP community 1 second host name or IP address - set** | Checks syntax and sets the second host name or IP address of community 1. | `snmp -c1i2` *hostname/ip_address*<br>where *hostname/ip_address* is the second host name or IP address of community 1.<br>• Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments.<br>• If this argument is not specified, the snmp command clears this option.<br>• You can also clear this option by assigning an empty string as its value.<br>This command can only be run by users who have one | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 71. snmp command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | | or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | |
| **SNMP community 1 third host name or IP address - set** | Checks syntax and sets the third host name or IP address of community 1. | `snmp -c1i3` *hostname/ip_ address*<br>where *hostname/ip_ address* is the third host name or IP address of community 1.<br>• Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments.<br>• If this argument is not specified, the snmp command clears this option.<br>• You can also clear this option by assigning an empty string as its value.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **SNMPv3 community 1 view type - set** | Sets the SNMPv3 view type for community 1. | `snmp -ca1` *type*<br>where *type* is<br>• `get`<br>• `set`<br>• `trap`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 71. snmp command (continued)

| Function | What it does | Command | Target *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **SNMP community 2 name - set** | Sets the name of community 2. | `snmp -c2` *name*<br>where *name* is a descriptive name of community 2.<br>• Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments.<br>• If this argument is not specified, the snmp command clears this option.<br>• You can also clear this option by assigning an empty string as its value.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **SNMP community 2 first host name or IP address - set** | Checks syntax and sets the first host name or IP address of community 2. | `snmp -c2i1` *hostname/ip_address*<br>where *hostname/ip_address* is the first host name or IP address of community 2.<br>• Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments.<br>• If this argument is not specified, the snmp command clears this option.<br>• You can also clear this option by assigning an empty string as its value.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 71. snmp command (continued)*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | | additional information. | |
| **SNMP community 2 second host name or IP address - set** | Checks syntax and sets the second host name or IP address of community 2. | `snmp -c2i2` *hostname/ip_ address*<br>where *hostname/ip_ address* is the second host name or IP address of community 2.<br>• Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments.<br>• If this argument is not specified, the snmp command clears this option.<br>• You can also clear this option by assigning an empty string as its value.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 71. snmp command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **SNMP community 2 third host name or IP address - set** | Checks syntax and sets the third host name or IP address of community 2. | `snmp -c2i3` *hostname/ip_address*<br>where *hostname/ip_address* is the third host name or IP address of community 2.<br>• Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments.<br>• If this argument is not specified, the snmp command clears this option.<br>• You can also clear this option by assigning an empty string as its value.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **SNMPv3 community 2 view type - set** | Sets the SNMPv3 view type for community 2. | `snmp -ca2` *type*<br>where *type* is<br>• `get`<br>• `set`<br>• `trap`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 71. snmp command (continued)

| Function | What it does | Command | **Target** *(see paths in* "Command targets" *on page 6)* |
|---|---|---|---|
| **SNMP community 3 name - set** | Sets the name of community 3. | `snmp -c3` *name*<br>where *name* is a descriptive name of community 3.<br>• Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments.<br>• If this argument is not specified, the snmp command clears this option.<br>• You can also clear this option by assigning an empty string as its value.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **SNMP community 3 first host name or IP address - set** | Checks syntax and sets the first host name or IP address of community 3. | `snmp -c3i1` *hostname/ip_address*<br>where *hostname/ip_address* is the first host name or IP address of community 3.<br>• Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments.<br>• If this argument is not specified, the snmp command clears this option.<br>• You can also clear this option by assigning an empty string as its value.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 71. snmp command (continued)*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | | additional information. | |
| **SNMP community 3 second host name or IP address - set** | Checks syntax and sets the second host name or IP address of community 3. | `snmp -c3i2` *hostname/ip_address*<br>where *hostname/ip_address* is the second host name or IP address of community 3.<br>• Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments.<br>• If this argument is not specified, the snmp command clears this option.<br>• You can also clear this option by assigning an empty string as its value.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 71. snmp command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **SNMP community 3 third host name or IP address - set** | Checks syntax and sets the third host name or IP address of community 3. | `snmp -c3i3` *hostname/ip_address*<br>where *hostname/ip_address* is the third host name or IP address of community 3.<br>• Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments.<br>• If this argument is not specified, the snmp command clears this option.<br>• You can also clear this option by assigning an empty string as its value.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **SNMPv3 community 3 view type - set** | Sets the SNMPv3 view type for community 3. | `snmp -ca3` *type*<br>where *type* is<br>• `get`<br>• `set`<br>• `trap`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 71. snmp command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **SNMP contact name - set** | Sets the contact name. | `snmp -cn` *contact_name*<br>where *contact_name* is the name of the party to be contacted when SNMP traps an event.<br>• Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments.<br>• If this argument is not specified, the snmp command clears this option.<br>• You can also clear this option by assigning an empty string as its value.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **SNMP location - set** | Sets the location. | `snmp -l` *hostname/ip_address*<br>where *hostname/ip_address* identifies the website supporting SNMP for this CMM.<br>• Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments.<br>• If this argument is not specified, the snmp command clears this option.<br>• You can also clear this option by assigning an empty string as its value.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 71. snmp command (continued)*

| Function | What it does | Command | **Target** *(see paths in* "Command targets" *on page 6)* |
|---|---|---|---|
|  |  | authority" on page 10 for additional information. |  |

**Example:** To view the SNMP configuration, while the primary CMM in bay 1 is set as the persistent command environment, at the system:mm[1]> prompt, type

```
snmp
```

To enable the SNMP agent and SNMP traps, while the primary CMM in bay 1 is set as the persistent command environment, at the system:mm[1]> prompt, type

```
snmp -a -on -t -on
```

The following example shows the information that is returned from these two commands:

```
system:mm[1]> snmp
-a Enabled
-a3 Enabled
-t Enabled
-l Raleigh,NC
-cn Mr. Smith
-c1 public
-c1i1 9.44.146.157
-c1i2 9.44.147.24
-c1i3 9.49.165.217
-ca1 set
-c2 private
-c2i1 9.42.226.4
-c2i2
-c2i3
-ca2 get
-c3 test
-c3i1 9.44.247.64
-c3i2
-c3i3
-ca3 getsystem:mm[1]> snmp -a -on -t -on
system:mm[1]>
```

## sol command

This command configures SOL (serial over LAN) functions and indicates SOL status.

**Note:** You access the compute node Integrated Management Module (IMM) CLI using a CMM SOL session (see "Starting an SOL session" on page 28). If no user accounts have been manually set up for the IMM of a compute node, connection to that IMM must be done using the current CMM user ID and password. In order for an IMM to communicate with the compute node Advanced Settings Utility (ASU) and UpdateXpress System Pack Installer (UXSPI) programs, a local user account must be set up for the compute node IMM. This local account is not included in an IMM configuration backup. For information about using the compute node IMM interface, see the compute node or IMM documentation.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "sol command errors" on page 463 for a list of error messages that are specific to the sol command.

*Table 72. sol command*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display SOL status** | Displays the SOL status for the targeted device:<br>• When the command target is the primary CMM, it displays the following values:<br>– -status *on/off* (global SOL status)<br>– -c *retry_count*<br>– -e *CLI_key_sequence*<br>– -i *retry_interval*<br>– -r *reset_blade_key_seq*<br>– -s *send_threshold*<br>– -t *accumulate_timeout*<br>• When the command target is a compute node, it displays the following:<br>– -status *enabled/disabled* (SOL status for the compute node)<br>– Status of any SOL sessions for that compute node:<br>– Not ready<br>– Ready<br>– Active<br>– SOL retry interval<br>– SOL retry count<br>– SOL bytes sent<br>– SOL bytes received<br>– SOL destination IP address (IPv6 format)<br>– SOL destination MAC address<br>– SOL console user ID<br>– SOL console login IP address<br>– SOL console session start time<br>– SOL console session stop time<br>– Compute node power state | `sol` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number.<br>Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |
| **SOL retry interval - set** | Sets the SOL retry interval to the input value. | `sol -i` *value*<br>where *value* is from 10 ms to 2550 ms, inclusive, in 10 ms increments. If you enter a value less than 10 ms, the retry interval will be set to 10 ms. If you enter a value greater than 2550 ms, the retry interval will be set to 2550 ms.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 72. sol command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | | • Blade configuration<br>See "Commands and user authority" on page 10 for additional information. | |
| **SOL retry count - set** | Sets the SOL retry count to the input value. | `sol -c` *value*<br>where *value* is from 0 to 7, inclusive. If you enter a value of 0, no retries will be attempted. If you enter a value greater than 7, an error will be displayed.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>• Blade configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **SOL send threshold - set** | Sets the SOL send threshold to the input value. Setting the threshold value to 1 causes the compute node system-management processor to send an SOL packet as soon as the first character is received. | `sol -s` *value*<br>where *value* is from 1 to 251, inclusive. If you enter a value outside this range, an error will be displayed.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>• Blade configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 72. sol command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **SOL accumulate timeout - set** | Sets the SOL accumulate timeout to the input value. | `sol -t` *value*<br>where *value* is from 5 ms to 1275 ms, inclusive. If you enter a value less than 5 ms, the accumulate timeout will be set to 5 ms. If you enter a value greater than 1275 ms, an error will be displayed.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>• Blade configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **SOL enable - global** | Enables SOL globally for the Lenovo Flex System chassis. The global SOL enable command does not affect the SOL session status for each compute node. | `sol -status enabled`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>• Blade configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **SOL enable - compute node** | Enables SOL for the specified compute node. | `sol -status enabled`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>• Blade configuration<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[`*x*`]`<br>where *x* is the node bay number. |

Table 72. sol command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **SOL disable - global** | Disables SOL globally for the Lenovo Flex System chassis. The global SOL disable command does not affect the SOL session status for each compute node. | `sol -status disabled`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>• Blade configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[x]`<br>where *x* is the primary CMM bay number. |
| **SOL disable - compute node** | Disables SOL for the specified compute node. | `sol -status disabled`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>• Blade configuration<br>See "Commands and user authority" on page 10 for additional information. | Compute node:<br>`blade[x]`<br>where *x* is the node bay number. |

*Table 72. sol command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **CLI key sequence - set** | Sets the key sequence that is used to enter the CLI while a Telnet session in SOL mode. | `sol -e` *value*<br>where *value* is the key sequence. In this sequence, a `^` (the carat symbol) indicates a Ctrl that maps to control-key sequences; for example:<br>• `^[` (the carat symbol followed by a left bracket) means `Esc`<br>• `^M` (the carat symbol followed by a capitol M) means carriage return.<br>Refer to an ASCII-to-key conversion table for a complete listing of control-key sequences.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>• Blade configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Reset compute node key sequence - set** | Sets the key sequence that will reset a compute node while a Telnet session in SOL mode. | `sol -r` *value*<br>where *value* is the key sequence. In this sequence, a ^ (the carat symbol) indicates a Ctrl that maps to control-key sequences; for example:<br>• `^[` (the carat symbol followed by a left bracket) means `Esc`<br>• `^M` (the carat symbol followed by a capitol M) means carriage return.<br>Refer to an ASCII-to-key conversion table for a complete listing of control-key sequences.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 72. sol command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | | • Chassis configuration<br>• Blade configuration<br>See "Commands and user authority" on page 10 for additional information. | |

**Example:**

To set the SOL accumulate timeout to 25 ms, while the primary CMM in bay 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type
```
sol -t 25
```

To set the reset compute node key sequence to Esc R Esc r Esc R, while the primary CMM in bay 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type
```
sol -r ^[R^[r^[R
```

To display the SOL settings for the CMM, while the primary CMM in bay 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type
```
sol
```

The following example shows the information that is returned from these commands:

```
system:mm[1]> sol -t 25
OK
system:mm[1]> sol -r ^[R^[r^[R
OK
system:mm[1]> sol
-status enabled
-c 3
-e ^[(
-i 250
-r ^[R^[r^[R
-s 250
-t 25
system:mm[1]>
```

To display the SOL settings for the compute node in the third bay, while compute node 3 is set as the persistent command environment, at the `system:blade[3]>` prompt, type
```
sol
```

The following example shows the information that is returned from this command:

```
system:blade[3]> sol
-status enabled
SOL Session: Ready
SOL retry interval: 64000 ms
SOL retry count: 7
SOL bytes sent: 0
SOL bytes received: 0
SOL destination IP address: FE80::3BA7:94FF:FE07:CBD0
SOL destination MAC: unknown
SOL console user ID:
SOL console login from:
```

```
SOL console session started:
SOL console session stopped:
Blade power state: On
system:blade[3]>
```

## sshcfg command

This command sets and displays the SSH and SFTP status of the CMM.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "sshcfg command errors" on page 464 for a list of error messages that are specific to the sshcfg command.

*Table 73. sshcfg command*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display SSH status** | Displays the SSH status of the CMM. Returned values are:<br>• -cstatus: state of CLI SSH server (enabled, disabled)<br>• -sftpstatus: state of secure FTP server (enabled, disabled)<br>• CLI SSH port number<br>• ssh-dss fingerprint<br>• ssh-rsa fingerprint<br>• number of SSH public keys installed<br>• number of locations available to store SSH keys<br>**Note:** For scripting purposes, the "-v1 off" state is always displayed. | `sshcfg` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Display RSA host key information** | Displays RSA host key information for the CMM. | `sshcfg -hk rsa` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Display DSA host key information** | Displays DSA host key information for the CMM. | `sshcfg -hk dsa` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 73. sshcfg command (continued)*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Generate host key** | Generates a host key for the CMM. | `sshcfg -hk gen`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set state of CLI SSH server** | Sets the state of the CLI SSH server for the CMM. | `sshcfg -cstatus` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set state of CLI SFTP server** | Sets the state of the CLI secure FTP (SFTP) server for the CMM. | `sshcfg -sftpstatus` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

**Example:**

To display SSH status, while the primary CMM in bay 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type
`sshcfg`

The following example shows the information that is returned from this command:

```
system:mm[1]> sshcfg
-v1 off
-cstatus enabled
-sftpstatus enabled
CLI SSH port 22
```

```
ssh-dss 1024 bit fingerprint: ac:8b:1d:65:7a:1a:99:66:17:11:13:7e:ee:5c:4b:4e
ssh-rsa 2048 bit fingerprint: ef:28:85:ae:4f:0d:a7:5f:17:44:01:44:9e:ff:4b:4b
0 SSH public keys installed
32 locations available to store SSH public keys
system:mm[1]>
```

## sslcfg command

This command sets and displays the Secure Sockets Layer (SSL) status of the CMM.

**Notes:**

- When the CMM is set to “Secure” security mode, only secure file transfer methods, such as HTTPS and SFTP, can be used for tasks involving file transfer when the CMM is acting as a server. Unsecure file transfer protocols, such as HTTP, FTP, and TFTP, are disabled when the CMM is acting as a server when the security mode is set to “Secure”. Unsecure file transfer protocols remain available for a CMM acting as a client for all commands when the security mode is set to “Secure”.
- For information about how to specify a URL for file transfer, see “Specifying a URL for file transfer” on page 29 in the *Lenovo Chassis Management Module 2 Command-Line Interface Reference Guide*.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See “Common errors” on page 407 for a list of error messages that apply to all commands or “sslcfg command errors” on page 465 for a list of error messages that are specific to the sslcfg command.

*Table 74. sslcfg command*

| **Function** | **What it does** | **Command** | **Target** *(see paths in “*Command targets*” on page 6)* |
|---|---|---|---|
| **Display CMM SSL status** | Displays the SSL status of the specified CMM. This status includes information about SSL certificates. | `sslcfg` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set SSL (secure LDAP) state for LDAP client** | Enables or disables SSL (secure LDAP) or starts transport layer security for the LDAP client.<br>**Notes:**<br>• By default, the LDAP client uses the same SSL certificate as the LDAP server.<br>• The LDAP client can be enabled if a certificate is in place. | `sslcfg -client` *state*<br>where *state* is `enabled` , `disabled` , or `starttls` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See “Commands and user authority” on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 74. sslcfg command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set SSL state for HTTPS server** | Enables or disables the HTTPS server.<br>**Note:** The HTTPS server can be enabled if a certificate is in place. | `sslcfg -server` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **View internally signed certificate** | Displays internally signed server certificate. | `sslcfg -view intsrv` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **View self-signed certificate** | Displays a certificate authority self-signed root certificate for the CMM. | `sslcfg -view ca` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 74. sslcfg command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Generate self-signed certificate** | Generates a self-signed certificate for the chassis certificate authority.<br>**Notes:**<br>- If a user executes this command, it will cause all certificates in the chassis to be re-signed. This means that any applications configured to trust certificates in the chassis will no longer trust those certificates. The user should export the new CA certificate and import it into the companion applications so that these applications can continue to manage the chassis. If users had imported the previous CA certificate into a web browser or any other application, they would want to replace it with the new certificate. Additionally, some security configuration artifacts that are signed by the CA certificate might be reprovisioned to the compute nodes.<br>- If the `crypto -m` option is set to `comp`, for compatibility with all NIST cipher suites (see the "crypto command" on page 110 for more information), the `sslcfg -gen ca -csa` certificate type option must be specified when generating a CA certificate.<br>- If the `crypto -m` option is set to `nist800-131a` (see the "crypto command" on page 110 for more information), the `sslcfg -gen ca -csa` option is optional; if it is specified, the certificate type must be set to `rsa2048sha256`. | `sslcfg -gen ca -csa` *type*<br>where the optional certificate *type* is:<br>- rsa2048sha1<br>- rsa2048sha256<br><br>This command can only be run by users who have one or more of the following command authorities:<br>- Supervisor<br>- Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **View externally signed server certificate** | Displays externally signed certificate information for the server. | `sslcfg -view extsrv` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 74. sslcfg command (continued)

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Import (upload) externally signed LDAP client certificate and CA bundle** | Import (upload) externally signed LDAP certificate and CA bundle for the LDAP client.<br>The upload locations of the externally signed certificate file and CA bundle are set separately using the `-u` and `-cabu` command options. | `sslcfg -upld -t client -u` *URL* `-cabu` *CA_URL*<br>where:<br>• *URL* is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the certificate file is located.<br>• *CA_URL* is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the certificate bundle is located.<br>**Note:** The `-t client` option is optional. If it is not specified, the command defaults to the client target.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Delete externally signed LDAP client certificate and CA bundle** | Remove an externally signed LDAP certificate and CA bundle from the LDAP client. | `sslcfg -remove -t client`<br>**Note:** The `-t client` option is optional. If it is not specified, the command defaults to the client target.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 74. sslcfg command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **View CA bundle for externally signed server certificate** | Displays certificate authority bundle information for the externally signed certificate of the server. | `sslcfg -view extcab` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Import (upload) externally signed server certificate and CA bundle** | Import (upload) externally signed certificate and CA bundle for the server.<br>The upload locations of the externally signed certificate file and CA bundle are set separately using the `-u` and `-cabu` command options. | `sslcfg -upld -t server -u` *URL* `-cabu` *CA_URL*<br>where:<br>• *URL* is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the certificate file is located.<br>• *CA_URL* is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the certificate bundle is located.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Reapply externally signed server certificate** | Reapply an externally signed server certificate to the LDAP server. Unsuccessful certificate application lists any compute nodes that are unable to use externally signed certificates: the CMM uses a self-signed certificate for the LDAP server in this case. | `sslcfg -reapply`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 74. sslcfg command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Generate self-signed certificate (for failed externally signed server certificate)** | Generates a self-signed certificate for use with an LDAP server that does not support externally signed server certificates.<br>The CMM LDAP server receives an SSL certificate internally signed by the CMM root certificate authority (CA) certificate. The IMM in each compute node then uses the root certificate in the LDAP client to trust the CMM LDAP server.<br>**Notes:**<br>• If a user executes this command, it will cause all certificates in the chassis to be re-signed. This means that any applications configured to trust certificates in the chassis will no longer trust those certificates. The user should export the new CA certificate and import it into the companion applications so that these applications can continue to manage the chassis. If users had imported the previous CA certificate into a web browser or any other application, they would want to replace it with the new certificate. Additionally, some security configuration artifacts that are signed by the CA certificate might be reprovisioned to the compute nodes.<br>• If the `crypto -m` option is set to `comp`, for compatibility with all NIST cipher suites (see the "crypto command" on page 110 for more information), the `sslcfg -gen ca -csa` certificate type option must be specified when generating a CA certificate.<br>• If the `crypto -m` option is set to `nist800-131a` (see the "crypto command" on page 110 for more information), the `sslcfg -gen ca -csa` option is optional; if it is specified, the certificate type must be set to `rsa2048sha256`. | `sslcfg -gen ldapsrv -csa` *type*<br>where the optional certificate *type* is:<br>• rsa2048sha1<br>• rsa2048sha256<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **View externally signed LDAP client certificate** | Displays externally signed LDAP client certificate information. | `sslcfg -view extclnt` | |

*Table 74. sslcfg command (continued)*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Generate CSR** | Generates a certificate signing request (CSR) for the CMM HTTPS server or LDAP client.<br>The following values must be set when generating a CSR:<br>• Country using the `-c` command option.<br>• State or province using the `-sp` command option.<br>• City or locality using the `-cl` command option.<br>• Organization name using the `-on` command option.<br>• CMM host name using the `-hn` command option.<br>**Note:** This host name must match the host name that is used by a web browser to connect to the CMM.<br>The following optional values can be set when generating a CSR:<br>• Contact person using the `-cp` command option.<br>• Email address of the contact person using the `-ea` command option.<br>• Unit within a company or organization using the `-ou` command option.<br>• Additional information such as a surname using the `-s` command option.<br>• Additional information such as a given name using the `-gn` command option.<br>• Additional information such as a initials using the `-in` command option.<br>• Additional information such as a distinguished name qualifier using the `-dq` command option.<br>• Additional information such as a CSR password using the `-cpwd` command option.<br>• Additional information such as an unstructured name qualifier using the `-un` command option. | `sslcfg -gen csr -c` *country* `-sp` "*state*"`-cl` "*city*"`-on` "*org*"`-hn` *hostname* `-cp` "*name*"`-ea` *email*`-ou` "*org_unit*"`-s` "*surname*" `-gn` "*given_name*"`-in` "*initial*"`-dq` "*dn_qualifier*"`-cpwd` *password*`-un` "*un_name*" `-t` *target*<br>where the following required options are:<br>• *country* is two-character alphabetic code for the country.<br>• "*state*" is a state or province name of up to 60 characters in length.<br>• "*city*" is a city or locality name of up to 50 characters in length.<br>• "*org*" is an organization name of up to 60 characters in length.<br>• *hostname* is a valid host name of up to 60 characters in length.<br>• *target* is `server` or `client`<br>where the following optional options are:<br>• "*name*" is up to 60 characters in length.<br>• *email* is a valid email address of up to 60 characters.<br>• "*org_unit*" is up to 60 characters.<br>• "*surname*" is up to 60 characters.<br>*(continued on next page)* | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Generate CSR** *(continued)* | | • "*given_name*" is up to 60 characters.<br>• "*initial*" is up to 20 characters.<br>• "*dn_qualifier*" is up to 60 characters. | |

*Table 74. sslcfg command (continued)*

| **Function** | **What it does** | **Command** | **Target** *(see paths in “Command targets” on page 6)* |
|---|---|---|---|
| | | • *password* is between 6 and 30 characters.<br>• "*un_name*" is up to 60 characters.<br>**Note:** Arguments that must be quote-delimited are shown in quotation marks.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See “Commands and user authority” on page 10 for additional information. | |
| **Download CA self-signed root certificate file** | Downloads the specified CA self-signed root certificate file.<br>The location of the CA self-signed root certificate file, including IP address of the server for downloading and filename, and must be set using the `-u` command option.<br>**Note:** To successfully download and import a CA certificate into an external LDAP server trust store, make sure that secure LDAP is enabled using the `sslcfg -server enabled` or the `sslcfg -client enabled` command. | `sslcfg -dnld ca -u` *URL*<br>where *URL* is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the certificate file is located.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See “Commands and user authority” on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 74. sslcfg command (continued)*

| Function | What it does | Command | **Target** *(see paths in "*Command targets*" on page 6)* |
|---|---|---|---|
| **Download certificate or CSR file of specified format** | Downloads the specified certificate file, specifying the certificate file format.<br>The location of the certificate or CSR file, including IP address of the server for downloading and filename, and must be set using the `-u` command option.<br>**Note:** If the certificate or CSR file format is not specified using the `-f` command option, the format defaults to DER. | `sslcfg -dnld` *cert_type*`-f` *format*`-u` *URL* `-t` *target*<br>where:<br>• *cert_type* is<br>– `cert` for a certificate<br>– `csr` for a CSR (for the CMM LDAP client certificate)<br>• *format* is<br>– `der` for binary DER encoded certificates<br>– `pem` for X.509v3 files that contain ASCII (Base64) armored data prefixed with a BEGIN line<br>• *URL* is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the certificate file is located.<br>• *target* is `server` or `client`<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **View trusted certificate 1** | Displays trusted certificate 1 information for the LDAP client. | `sslcfg -tc1 view` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **View trusted certificate 2** | Displays trusted certificate 2 information for the LDAP client. | `sslcfg -tc2 view` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 74. sslcfg command (continued)

| Function | What it does | Command | Target *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **View trusted certificate 3** | Displays trusted certificate 3 information for the LDAP client. | `sslcfg -tc3 view` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[x]`<br>where *x* is the primary CMM bay number. |
| **Import (upload) trusted certificate 1** | Import (upload) trusted certificate 1 for the LDAP client.<br>The upload location of the trusted certificate file, including IP address of the server and filename, an must be set using the `-u` command option. | `sslcfg -tc1 import -u` *URL* `-t client`<br>where *URL* is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the certificate file is located.<br>**Note:** The `-t client` option is optional. If it is not specified, the command defaults to the client target.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[x]`<br>where *x* is the primary CMM bay number. |

*Table 74. sslcfg command (continued)*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "*Command targets*" on page 6)* |
|---|---|---|---|
| **Import (upload) trusted certificate 2** | Import (upload) trusted certificate 2 for the LDAP client.<br>The upload location of the trusted certificate file, including IP address of the server and filename, an must be set using the `-u` command option. | `sslcfg -tc2 import -u` *URL* `-t client`<br>where *URL* is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the certificate file is located.<br>**Note:** The `-t client` option is optional. If it is not specified, the command defaults to the client target.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Import (upload) trusted certificate 3** | Import (upload) trusted certificate 3 for the LDAP client.<br>The upload location of the trusted certificate file, including IP address of the server and filename, an must be set using the `-u` command option. | `sslcfg -tc3 import -u` *URL* `-t client`<br>where *URL* is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the certificate file is located.<br>**Note:** The `-t client` option is optional. If it is not specified, the command defaults to the client target.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 74. sslcfg command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Export (download) trusted certificate 1** | Downloads (exports) trusted certificate 1 for the LDAP client. The location of the trusted certificate 1 file, including IP address of the server for downloading and filename, and must be set using the -u command option. | `sslcfg -tc1 download -u` *URL* `-t client`<br>where *URL* is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the certificate file is located.<br>**Note:** The `-t client` option is optional. If it is not specified, the command defaults to the client target.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Export (download) trusted certificate 2** | Downloads (exports) trusted certificate 2 for the LDAP client. The location of the trusted certificate 2 file, including IP address of the server for downloading and filename, and must be set using the -u command option. | `sslcfg -tc2 download -u` *URL* `-t client`<br>where *URL* is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the certificate file is located.<br>**Note:** The `-t client` option is optional. If it is not specified, the command defaults to the client target.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 74. sslcfg command (continued)

| Function | What it does | Command | Target *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Export (download) trusted certificate 3** | Downloads (exports) trusted certificate 3 for the LDAP client. The location of the trusted certificate 3 file, including IP address of the server for downloading and filename, and must be set using the -u command option. | `sslcfg -tc3 download -u` *URL* `-t client`<br>where *URL* is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the certificate file is located.<br>**Note:** The `-t client` option is optional. If it is not specified, the command defaults to the client target.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Remove trusted certificate 1** | Removes trusted certificate 1 from the LDAP client. | `sslcfg -tc1 remove -t client`<br>**Note:** The `-t client` option is optional. If it is not specified, the command defaults to the client target.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 74. sslcfg command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Remove trusted certificate 2** | Removes trusted certificate 2 from the LDAP client. | `sslcfg -tc2 remove -t client`<br>**Note:** The `-t client` option is optional. If it is not specified, the command defaults to the client target.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Remove trusted certificate 3** | Removes trusted certificate 3 from the LDAP client. | `sslcfg -tc3 remove -t client`<br>**Note:** The `-t client` option is optional. If it is not specified, the command defaults to the client target.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 74. sslcfg command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Import (upload) certificate** | Import (upload) certificate for the CMM HTTPS server or LDAP client. The upload location of the certificate file, including IP address and filename, an must be set using the `-u` command option. | `sslcfg -upld -u` *URL* `-t` *target*<br>where:<br>• *URL* is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the certificate file is located.<br>• *target* is `server` or `client`<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **View CRL 1** | Displays certificate revocation list 1 for the LDAP client. | `sslcfg -crl1 view` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **View CRL 2** | Displays certificate revocation list 2 for the LDAP client. | `sslcfg -crl2 view` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **View CRL 3** | Displays certificate revocation list 3 for the LDAP client. | `sslcfg -crl3 view` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 74. sslcfg command (continued)*

| Function | What it does | Command | **Target** *(see paths in “Command targets” on page 6)* |
|---|---|---|---|
| **Set CRL checking state for LDAP client** | Enables or disables certificate revocation list checking for the LDAP client. | `sslcfg -crl` *state*<br>where *state* is `enabled` or `disabled` .<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See “Commands and user authority” on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Import (upload) CRL 1** | Import (upload) certificate revocation list 1 for the LDAP client. The upload location of the CRL, including IP address of the server and filename, an must be set using the `-u` command option. | `sslcfg -crl1 import -u` *URL* `-t client`<br>where *URL* is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the CRL is located.<br>**Note:** The `-t client` option is optional. If it is not specified, the command defaults to the client target.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See “Commands and user authority” on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 74. sslcfg command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Import (upload) CRL 2** | Import (upload) certificate revocation list 2 for the LDAP client. The upload location of the CRL, including IP address of the server and filename, an must be set using the `-u` command option. | `sslcfg -crl2 import -u` *URL* `-t client`<br>where *URL* is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the CRL is located.<br>**Note:** The `-t client` option is optional. If it is not specified, the command defaults to the client target.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Import (upload) CRL 3** | Import (upload) certificate revocation list 3 for the LDAP client. The upload location of the CRL, including IP address of the server and filename, an must be set using the `-u` command option. | `sslcfg -crl3 import -u` *URL* `-t client`<br>where *URL* is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the CRL is located.<br>**Note:** The `-t client` option is optional. If it is not specified, the command defaults to the client target.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 74. sslcfg command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Remove CRL 1** | Removes certificate revocation list 1 from the LDAP client. | `sslcfg -crl1 remove -t client`<br>**Note:** The `-t client` option is optional. If it is not specified, the command defaults to the client target.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Remove CRL 2** | Removes certificate revocation list 2 from the LDAP client. | `sslcfg -crl2 remove -t client`<br>**Note:** The `-t client` option is optional. If it is not specified, the command defaults to the client target.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Remove CRL 3** | Removes certificate revocation list 3 from the LDAP client. | `sslcfg -crl3 remove -t client`<br>**Note:** The `-t client` option is optional. If it is not specified, the command defaults to the client target.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

**Example:** To view SSL information for the primary CMM in bay 1, while this CMM is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
sslcfg
```

To generate a new key and CSR for the server in the primary CMM in bay 1, with a country of US, a state of NC, a city of Cary, an organization of Lenovo, and a host name of hostname, while this CMM is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
sslcfg -gen csr -c us -sp "nc"  -cl "cary"  -on "lenovo" -hn hostname -t server
```

The following example shows the information that is returned from these commands:

```
system:mm[1]> sslcfg
-server enabled
-client disabled
Certificate Authority certificate status:
A Root certificate is installed (rsa2048sha1)
SSL Server Certificate status:
A self-signed certificate is installed
SSL Client Certificate status:
No certificate has been generated
SSL Client Trusted Certificate status:
Trusted Certificate 1: Not available
Trusted Certificate 2: Not available
Trusted Certificate 3: Not available
SSL Client CRL status:
CRL 1: Not available
CRL 2: Not available
CRL 3: Not available
-crl disabled
system:mm[1]>
system:mm[1]> sslcfg -gen csr -c us -sp "nc"  -cl "cary"  -on "lenovo" -hn hostname -t server
Certificate Signing Request (CSR) is ready for downloading.
To get the CSR, use the download CSR command. You can then send
it to a CA for signing.
OK
system:mm[1]>
```

## syslog command

This command manages how the CMM handles transmission of event log messages to networked syslog event collectors.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "syslog command errors" on page 469 for a list of error messages that are specific to the syslog command.

**Notes:**

- When using the syslog command to send CMM system event logs over a network, the data is sent unencrypted and can be read by any user that is connected to the network.
- The messages a CMM sends to the syslog server are facility 1 user-level messages. Each message is assigned a priority that is based on the severity of the event being converted.

*Table 75. syslog command*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display syslog configuration** | Displays the syslog event log transmission configuration of the CMM. | `syslog` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set syslog filter level** | Set severity filtering levels for syslog event log transmission. | `syslog -sev` *level*<br>where *level* is:<br>• `i` selects error, warning, and informational logs<br>• `w` selects error and warning logs<br>• `e` selects error logs<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>• Chassis log management<br>• Chassis administration<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set syslog event log transmission state for collector 1** | Enables or disables syslog event log transmission to collector 1. | `syslog -coll1` *state*<br>where *state* is `enabled` or `disabled`.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>• Chassis log management<br>• Chassis administration<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 75. syslog command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set syslog event log transmission state for collector 2** | Enables or disables syslog event log transmission to collector 2. | `syslog -coll2` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>• Chassis log management<br>• Chassis administration<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Syslog event log collector 1 host name or IP address - set** | Sets the host name or IP address for syslog event collector 1. | `syslog -i1` *hostname/ip_ address*<br>where *hostname/ip_ address* is the collector 1 host name or IP address.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>• Chassis log management<br>• Chassis administration<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 75. syslog command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Syslog event log collector 2 host name or IP address - set** | Sets the host name or IP address for syslog event collector 2. | `syslog -i2` *hostname/ip_address*<br>where *hostname/ip_address* is the collector 2 host name or IP address.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>• Chassis log management<br>• Chassis administration<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Syslog event log collector 1 port number - set** | Sets the port number for syslog event collector 1. | syslog -p1 *port*<br>where *port* is the collector 1 port number from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>• Chassis log management<br>• Chassis administration<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 75. syslog command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Syslog event log collector 2 port number - set** | Sets the port number for syslog event collector 2. | `syslog -p2` *port*<br>where *port* is the collector 2 port number from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>• Chassis log management<br>• Chassis administration<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Generate test message** | Generates a test syslog message to test the configuration.<br>**Note:** The -test command options must be run exclusive of other command options. | `syslog -test`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>• Chassis log management<br>• Chassis administration<br>• Chassis configuration<br>• Blade administration<br>• Blade configuration<br>• Blade remote presence<br>• I/O module administration<br>• I/O module configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| Set timestamp format | Set timestamp format for syslog event log transmission. | `syslog -f` *format*<br>where *format* is:<br>• default<br>where the timestamp format is like in this example<br>`'Thu Mar  1` | Primary CMM:<br>`-T system:mm[x]`<br>.<br>where *x* is the primary management-module bay number. |

*Table 75. syslog command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | | `07:42:53 2018'`<br>• RFC3164<br>where the timestamp format is complaint with RFC 3164. Example:<br>`'Mar 1 07:42:53'`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | |

**Example:** To view the syslog event log transmission configuration of the primary CMM in bay 1, while this CMM is set as the persistent command environment, at the `system:mm[1]>` prompt, type
`syslog`

The following example shows the information that is returned from this command:

```
system:mm[1]> syslog
-sev i
-coll1 enabled
-coll2 enabled
-i1 10.241.53.60
-i2 10.241.53.41
-p1 514
-p2 514
-f default
system:mm[1]>
```

## tcpcmdmode command

This command displays and changes the timeout of the TCP command-mode sessions that are used by optional management devices, such as the Lenovo XClarity Administrator or Flex System Manager software, for out-of-band communication with the CMM. This command is also used to enable or disable the TCP command-mode sessions.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "tcpcmdmode command errors" on page 470 for a list of error messages that are specific to the tcpcmdmode command.

*Table 76. tcpcmdmode command*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display TCP command-mode session status and timeout** | Displays the secure and non-secure TCP command-mode session status (maximum number of sessions) and timeout. | `tcpcmdmode` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set TCP command-mode session timeout** | Sets the secure and non-secure TCP command-mode session timeout value. | `tcpcmdmode -t` *timeout*<br>where *timeout* is from 0 seconds (no timeout) to 4294967295 seconds, inclusive. If you enter a value outside this range, an error will be displayed.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Disable TCP command-mode sessions** | Disables TCP command-mode sessions that are used by optional management devices for out-of-band communication with the CMM. This applies to both read and write operations. | `tcpcmdmode -status 0`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 76. tcpcmdmode command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Enable and set number of TCP command-mode sessions** | Enables TCP command-mode and sets the maximum number of sessions that can be used by optional management devices for out-of-band communication with the CMM. For read operations, all of the values from 1 to 20, inclusive, mean *enabled*.<br>**Notes:**<br>• The CMM supports a combined total of up to 20 secure and non-secure TCP command-mode sessions.<br>• Non-secure TCP command-mode can not be enabled if the CMM chassis security level is set to secure with the "security command" on page 298. | `tcpcmdmode -status` *number_sessions*<br>where *number_sessions* is from 1 to 20, inclusive. (A value of 0 disables TCP command-mode sessions.) If you enter a value outside this range, an error will be displayed.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Disable secure TCP command-mode sessions** | Disables secure TCP command-mode sessions that are used by optional management devices for out-of-band communication with the CMM. This applies to both read and write operations. | `tcpcmdmode -sstatus 0`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Enable and set number of secure TCP command-mode sessions** | Enables secure TCP command-mode and sets the maximum number of sessions that can be used by optional management devices for out-of-band communication with the CMM. For read operations, all of the values from 1 to 20, inclusive, mean *enabled*.<br>**Note:** The CMM supports a combined total of up to 20 secure and non-secure TCP command-mode sessions. | `tcpcmdmode -sstatus` *number_sessions*<br>where *number_sessions* is from 1 to 20, inclusive. (A value of 0 disables secure TCP command-mode sessions.) If you enter a value outside this range, an error will be displayed.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

**Example:** To enable a maximum of five secure TCP command-mode sessions for the primary CMM, while the primary CMM in bay 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type

```
tcpcmdmode -sstatus 5
```

To set the TCP command-mode session timeout for the primary CMM to 6 minutes, while the primary CMM in bay 1 is set as the persistent command environment, at the system:mm[1]> prompt, type

```
tcpcmdmode -t 360
```

To display the TCP command-mode session status and timeout for the primary CMM, while the primary CMM in bay 1 is set as the persistent command environment, at the system:mm[1]> prompt, type

```
tcpcmdmode
```

The following example shows the information that is returned from these commands:

```
system:mm[1]> tcpcmdmode -sstatus 5
OK
system:mm[1]> tcpcmdmode -t 360
OK
system:mm[1]> tcpcmdmode
-sstatus 5 connections
-status 1 connection
-t 360 seconds
system:mm[1]>
```

## temps command

This command displays actual temperatures and temperature threshold values for Lenovo Flex System components.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "temps command errors" on page 470 for a list of error messages that are specific to the temps command.

*Table 77. temps command*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display temperature values** | Displays the current temperature and temperature threshold settings for the specified component:<br>• The compute node target displays the temperature values for components in the specified compute node, such as microprocessors and expansion modules.<br>• The rear LED card target displays values for the temperature sensor in the rear LED card. | `temps` | Compute node:<br>`blade[`*x*`]` where *x* is the node bay number.<br>Rear LED card:<br>`mt[`*x*`]` where *x* is the rear LED card. |

**Example:** To view the current temperature and temperature thresholds for the first compute node in the storage expansion enclosure in bay 11, while the Lenovo Flex System chassis is set as the persistent command environment, at the system> prompt, type

```
temps -T bladeenclosure[11]:blade[1]
```

The following example shows the information that is returned from this command:

```
system> temps -T bladeenclosure[11]:blade[1]
```

```
                                                   Hard    Warning
          Component              Value   Warning  Shutdown   Reset
----------------------------   -------  -------  --------  -------
Inlet Temp                     28.00    43.00    46.00     39.00
PIB Left Temp                  28.00    70.00    89.00     66.00
PIB Right Temp                 27.00    65.00    75.00     61.00
PCH Temp                        59.00    100.00   110.00    96.00
CPU Temp                        46.00    76.00    90.00     72.00
Battery Temp                   25.00    60.00    65.00     56.00
DIMM 1 Temp                     33.00    97.00    105.00    93.00
DIMM 2 Temp                     33.00    97.00    105.00    93.00
system>
```

## trespass command

This command sets and displays the status and message for the CMM trespass feature that can display a warning message to users when they log in.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "trespass command errors" on page 471 for a list of error messages that are specific to the trespass command.

*Table 78. trespass command*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display status of CMM trespass feature** | Displays status of the trespass feature for the CMM. Possible return values are:<br>• -twe (on or off)<br>• -tw *warning_message*<br>**Note:** The *warning_message* is shown only when the trespass feature is enabled (-twe on). | `trespass` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Enable / disable CMM trespass feature** | Enables or disables trespass feature for CMM. | `trespass -twe` *state*<br>where *state* is `on` or `off` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 78. trespass command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set CMM trespass message** | Sets message that is displayed to users who log in to the CMM when the trespass feature is enabled.<br>**Note:** Setting a new *warning_ message* permanently replaces the default warning message. | `trespass -tw` "*warning_ message*"<br>where "*warning_ message*" is up to 1600 characters in length and enclosed in double-quotation marks.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set CMM trespass feature to default values** | Sets trespass feature to default values:<br>• -twe: off<br>• -tw (warning message): WARNING! This computer system and network is PRIVATE AND PROPRIETARY and may only be accessed by authorized users. Unauthorized use of this computer system or network is strictly prohibited and may be subject to criminal prosecution, employee discipline up to and including discharge, or the termination of vendor/service contracts. The owner, or its agents , may monitor any activity or communication on the computer system or network. The owner, or its agents, may retrieve any information stored within the computer system or network. By accessing and using this computer system or network, you are consenting to such monitoring and information retrieval for law enforcement and other purposes. Users should have no expectation of privacy as to any communication on or information stored within the computer system or network, including information stored locally or remotely on a hard drive or other media in use with | `trespass -twd`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 78. trespass command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | this computer system or network. | | |

**Example:**

To enable the CMM trespass feature, while the primary CMM in bay 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type
`trespass -twe on`

To set the trespass feature message to 'Authorized Access only', while the primary CMM in bay 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type
`trespass -tw "Authorized Access only"`

To display the CMM trespass feature status, while the primary CMM in bay 1 is set as the persistent command environment, at the `system:mm[1]>` prompt, type
`trespass`

The following example shows the information that is returned from these commands:

```
system:mm[1]> trespass -twe on
OK
system:mm[1]> trespass -tw "Authorized Access only"
-tw OK
system:mm[1]> trespass
-twe on
-tw Authorized Access only
system:mm[1]>
```

## uicfg command

This command displays and configures the CMM user interface settings.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "uicfg command errors" on page 471 for a list of error messages that are specific to the uicfg command.

*Table 79. uicfg command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display CMM user interface settings** | Displays the user interface settings for the CMM. Returned values indicate enabled or disabled status for the following interfaces:<br>- -cim (common information model used by the optional Lenovo XClarity Administrator or Flex System Manager software)<br>- -cli (command line)<br>- -snmp<br>- -tcm (TCP command mode)<br>- -stcm (secure TCP command mode)<br>- -web (web interface) | `uicfg` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Enable / disable command-line interface** | Enables or disables the CMM command-line interface (using Telnet or SSH).<br>**Note:** The Telnet interface will not be available if the CMM chassis security level is set to secure with the "security command" on page 298. | `uicfg -cli` *state*<br>where *state* is `enabled` or `disabled`.<br>This command can only be run by users who have one or more of the following command authorities:<br>- Supervisor<br>- Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Enable / disable CIM** | Enables or disables the CMM common information model (CIM) interface used by the optional Lenovo XClarity Administrator or Flex System Manager software. | `uicfg -cim` *state*<br>where *state* is `enabled` or `disabled`.<br>This command can only be run by users who have one or more of the following command authorities:<br>- Supervisor<br>- Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 79. uicfg command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Enable / disable SNMPv1 and SNMPv3** | Enables or disables SNMPv1 and SNMPv3 connections to the CMM.<br>**Note:** SNMPv1 connections will not be available if the CMM chassis security level is set to secure with the "security command" on page 298. | `uicfg -snmp` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Disable or set number of TCP command mode connections** | Disable the TCP command mode (used by the optional Lenovo XClarity Administrator or Flex System Manager software) for the CMM, or explicitly set the maximum number of TCP command mode connections.<br>**Notes:**<br>• Any number of connections (1 through 20) displays a status of enabled. Zero connections displays a status of disabled.<br>• Non-secure TCM command mode will not be available if the CMM chassis security level is set to secure with the "security command" on page 298. | `uicfg -tcm` *port_mode*<br>where *port_mode* is:<br>• `disabled` (no connections)<br>• `enabled` (1 connection)<br>• a number between 0 and 20, inclusive, that indicates the maximum number of non-secure TCP session connections<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 79. uicfg command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Disable or set number of secure TCP command mode connections** | Disable the secure TCP command mode (used by the optional Flex System Manager software) for the CMM, or explicitly set the maximum number of secure TCP command mode connections.<br>**Notes:**<br>• On a write operation, the maximum number of connections can be set explicitly (0-20), or it can be enabled (1 connection) or disabled (0 connections).<br>• On a read operation, disabled means 0 connections, and enabled means 1 or more connections.<br>• The total session count of TCM and STCM is limited to 20. | uicfg -stcm *port_mode*<br>where *port_mode* is:<br>• disabled (no connections)<br>• enabled (1 connection)<br>• a number between 0 and 20, inclusive, that indicates the maximum number of secure TCP session connections<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>mm[p]<br>mm[P]<br>mm[*x*]<br>where *x* is the primary CMM bay number. |
| **Enable / disable web interface** | Enables or disables the CMM web interface. | uicfg -web *state*<br>where *state* is enabled or disabled .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>mm[p]<br>mm[P]<br>mm[*x*]<br>where *x* is the primary CMM bay number. |

**Example:** To disable the common information model for the CMM, while the primary CMM in bay 1 is set as the persistent command environment, at the system:mm[1]> prompt, type

```
uicfg -cim disabled
```

To display the user interface configuration for the CMM, while CMM 1 is set as the persistent command environment, at the system:mm[1]> prompt, type

```
uicfg
```

The following example shows the information that is returned from these two commands:

```
system:mm[1]> uicfg -cim disabled
Warning: Communication using the common information model
has been disabled.
OK
system:mm[1]> uicfg
-cim disabled
```

```
-cli enabled
-stcm disabled
system:mm[1]>
```

## update command

This command updates firmware using the uniform resource locator (URL) of a TFTP, FTP, HTTP, HTTPS, or SFTP server and displays information about firmware installed in Lenovo Flex System components.

**Attention:** Installing the wrong firmware update might cause the CMM to malfunction. Before you install a firmware update, read any readme and change history files that are provided with the downloaded update. These files contain important information about the update and the procedure for installing the update, including any special procedure for updating from an early firmware version to the latest version.

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

**Notes:**

- When the CMM is set to “Secure” security mode, only secure file transfer methods, such as HTTPS and SFTP, can be used for tasks involving file transfer when the CMM is acting as a server. Unsecure file transfer protocols, such as HTTP, FTP, and TFTP, are disabled when the CMM is acting as a server when the security mode is set to “Secure”. Unsecure file transfer protocols remain available for a CMM acting as a client for all commands when the security mode is set to “Secure”.
- For information about how to specify a URL for file transfer, see “Specifying a URL for file transfer” on page 29.
- The CMM update command does not support updating compute node firmware. If an optional management device, such as the Lenovo XClarity Administrator or Flex System Manager management server is installed in the Lenovo Flex System chassis, you can update compute node firmware using the management device program (see https://support.lenovo.com/solutions/HT116912). Depending on your compute node type, other methods are available for updating compute node firmware. See the documentation for your compute node for information.
- For additional information about updating firmware for Lenovo Flex System, see the *Firmware Update Best Practices Guide* athttps://support.lenovo.com/solutions/HT116912 (you might need to register to access this content).

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See “Common errors” on page 407 for a list of error messages that apply to all commands or “update command errors” on page 472 for a list of error messages that are specific to the update command.

*Table 80. update command*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display firmware attributes** | Displays attributes of the firmware installed in the command target.<br>Return values are:<br>• Firmware type<br>• Build ID<br>• Filename<br>• Release date<br>• Revision level<br>**Notes:**<br>• When the command target is the primary CMM, this command will return the values for the currently active firmware and for the pending firmware, that will become active after the next CMM reboot.<br>• For a standby CMM, the returned value will also indicate if a firmware update is in progress and the percentage that is complete.<br>• For I/O modules that support it, this command will also display firmware image information. | `update -a` | Primary or standby CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[s]`<br>`mm[S]`<br>`mm[`*x*`]`<br>where *x* is the primary or standby CMM bay number.<br>I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |
| **Update firmware using URL** | Update firmware for the command target using a uniform resource locator (URL).<br>**Attention:**<br>• Installing the wrong firmware update might cause the CMM to malfunction.<br>**Important:** Command authority definitions might change between firmware versions. Make sure that the command authority level set for each user is correct after updating CMM firmware (see "Commands and user authority" on page 10).<br>**Notes:**<br>• Updating to older firmware levels may cause loss of certain functionality.<br>• When the primary CMM firmware image is updated, the "old" primary image becomes the "new" backup image. These changes do not take effect until the CMM is rebooted.<br>• Some I/O modules support only RSA fingerprinting when updating through SFTP. See the | `update -u` *URL*<br>where *URL* is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the firmware update image is located.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis administration (for CMM)<br>• I/O module administration (for I/O module)<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number.<br>I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |

*Table 80. update command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | documentation that comes with your I/O module for information. | | |
| **Update firmware and reboot** | Update firmware and reboot the CMM to use new firmware if the update succeeds.<br>**Attention:**<br>• Installing the wrong firmware update might cause the CMM to malfunction.<br>**Important:** Command authority definitions might change between firmware versions. Make sure that the command authority level set for each user is correct after updating CMM firmware.<br>**Note:** When the primary CMM firmware image is updated, the "old" primary image becomes the "new" backup image. These changes do not take effect until the CMM is rebooted. | `update -u` *URL* `-r`<br>where *URL* is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the firmware update image is located.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis administration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 80. update command (continued)

| Function | What it does | Command | Target (see paths in "Command targets" on page 6) |
|---|---|---|---|
| **Update firmware (verbose)** | Update firmware for the command target, showing details of the firmware download and flash operations. The detailed information is not shown until the update is complete, which might take several minutes.<br>**Attention:**<br>• Installing the wrong firmware update might cause the CMM to malfunction.<br>**Important:** Command authority definitions might change between firmware versions. Make sure that the command authority level set for each user is correct after updating CMM firmware.<br>**Notes:**<br>• Updating to older firmware levels may cause loss of certain functionality.<br>• When the primary CMM firmware image is updated, the "old" primary image becomes the "new" backup image. These changes do not take effect until the CMM is rebooted.<br>• Some I/O modules support only RSA fingerprinting when updating through SFTP. See the documentation that comes with your I/O module for information. | `update -u` *URL* `-v`<br>where *URL* is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the firmware update image is located.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis administration (for CMM)<br>• I/O module administration (for I/O module)<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number.<br>I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |
| **Update I/O module firmware** | Directly update I/O module firmware image.<br>**Attention:** Installing the wrong firmware update might cause the I/O module to malfunction. Before you install a firmware update, read any readme and change history files that are provided with the downloaded update. These files contain important information about the update and the procedure for installing the update, including any special procedure for updating from an early firmware version to the latest version.<br>**Notes:**<br>• Only some I/O modules have this capability. | `update -u` *URL* `-img` *img_index*<br>where:<br>• *URL* is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the firmware update image is located.<br>• *img_index* is the image index you are updating. Use the `update -a` command to list available images and their index numbers. | I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |

Table 80. update command (continued)

| Function | What it does | Command | **Target** *(see paths in "*Command targets*" on page 6)* |
|---|---|---|---|
| | • Some I/O modules support only RSA fingerprinting when updating through SFTP. See the documentation that comes with your I/O module for information. | This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• I/O module administration<br>See "Commands and user authority" on page 10 for additional information. | |
| **Update I/O module firmware (verbose)** | Directly update I/O module firmware image, showing details of the firmware download and flash operations. The detailed information is not shown until the update is complete, which might take several minutes.<br>**Attention:** Installing the wrong firmware update might cause the I/O module to malfunction. Before you install a firmware update, read any readme and change history files that are provided with the downloaded update. These files contain important information about the update and the procedure for installing the update, including any special procedure for updating from an early firmware version to the latest version.<br>**Notes:**<br>• Only some I/O modules have this capability.<br>• Some I/O modules support only RSA fingerprinting when updating through SFTP. See the documentation that comes with your I/O module for information. | `update -u` *URL* `-img` *img_index* `-v`<br>where:<br>• *URL* is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the firmware update image is located.<br>• *img_index* is the image index to the I/O module firmware you are updating. Use the `update -a` command to list available images and their index numbers.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• I/O module administration<br>See "Commands and user authority" on page 10 for additional information. | I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |

*Table 80. update command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Activate I/O module firmware** | Directly activate I/O module firmware image.<br>**Note:** Only some I/O modules have this capability. | `update -activate` *img_index*<br>where *img_index* is the image index you are activating. Use the `update -a` command to list available images and their index numbers.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• I/O module administration<br>See "Commands and user authority" on page 10 for additional information. | I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |
| **Update and activate I/O module firmware** | Directly update I/O module and activate the firmware image.<br>**Attention:** Installing the wrong firmware update might cause the I/O module to malfunction. Before you install a firmware update, read any readme and change history files that are provided with the downloaded update. These files contain important information about the update and the procedure for installing the update, including any special procedure for updating from an early firmware version to the latest version.<br><br>**Notes:**<br>• Only some I/O modules have this capability.<br>• The activate option can be used with the other options. You can flash first, then activate the specified index.<br>• The image index you activate can be different from the one you update.<br>• Some I/O modules support only RSA fingerprinting when updating through SFTP. See the documentation that comes with your I/O module for information. | `update -u` *URL*`-img` *img_index*`-activate` *img_index*<br>where:<br>• *URL* is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the firmware update image is located.<br>• *img_index* is the image index you are activating. Use the `update -a` command to list available images and their index numbers.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• I/O module administration<br>See "Commands and user authority" on page 10 for additional information. | I/O module:<br>`switch[`*x*`]`<br>where *x* is the I/O-bay number. |

**Example:** To update the CMM firmware from a HTTP server and reboot the primary CMM in bay 2 after a successful update, while the Lenovo Flex System chassis is set as the persistent command environment, type the following command at the `system:>` prompt. For this example, the IP address of the HTTP server is 10.12.100.109 and the firmware file containing the update is named cmefs.uxp that is in the flash sub-directory on the server. The verbose mode and reboot flag are also specified.

```
update -u http://10.12.100.109/flash/cmefs.uxp -T mm[p] -v -r
```

The following example shows the information that is returned from the update command:

```
system> update -u http://10.12.100.109/flash/cmefs.uxp -T mm[p] -v -r
Flashing firmware to target device
Starting flash packet preparation.
Flash operation phase starting.
Flashing - packet percent complete 0.
Flashing - packet percent complete 0.
Flashing - packet percent complete 25.
Flashing - packet percent complete 25.
Flashing - packet percent complete 25.
Flashing - packet percent complete 25.
Flashing - packet percent complete 25.
Flashing - packet percent complete 70.
Flashing - packet percent complete 70.
Flashing - packet percent complete 70.
Flashing - packet percent complete 70.
Flashing - packet percent complete 90.
Flashing - packet percent complete 90.
Flashing - packet percent complete 90.
Flashing - packet percent complete 90.
Flashing - packet percent complete 90.
Flashing - packet percent complete 90.
Flashing - packet percent complete 90.
Flashing - packet percent complete 90.
Flashing - packet percent complete 90.
Flashing - packet percent complete 90.
Flashing - packet percent complete 90.
Flashing - packet percent complete 90.
Flashing - packet percent complete 90.
Flashing - packet percent complete 90.
Flashing - packet percent complete 90.
Flashing - packet percent complete 90.
successful
The new firmware will become active after the next reset of the MM.

Rebooting MM...
system>

system> update -T switch[3] -u sftp://USERID:Passw0rd@172.20.25.10/tftproot/v8.1.0b_pha/ -img 1 -v
Flashing firmware to target device
Starting flash packet preparation.
Flash operation phase starting.
Flashing - packet percent complete 0.
Flashing - packet percent complete 0.
Flashing - packet percent complete 25.
Flashing - packet percent complete 25.
Flashing - packet percent complete 25.
Flashing - packet percent complete 25.
Flashing - packet percent complete 25.
Flashing - packet percent complete 70.
Flashing - packet percent complete 70.
Flashing - packet percent complete 70.
Flashing - packet percent complete 70.
Flashing - packet percent complete 90.
Flashing - packet percent complete 90.
Flashing - packet percent complete 90.
Flashing - packet percent complete 90.
Flashing - packet percent complete 90.
Flashing - packet percent complete 90.
Flashing - packet percent complete 90.
Flashing - packet percent complete 90.
Flashing - packet percent complete 90.
Flashing - packet percent complete 90.
Flashing - packet percent complete 90.
Flashing - packet percent complete 90.
Flashing - packet percent complete 90.
Flashing - packet percent complete 90.
Flashing - packet percent complete 90.
Flashing - packet percent complete 90.
successful
The new firmware will become active after the next reset of the IOM.

Rebooting IOM...
system>
```

## uplink command

This command displays and configures the CMM uplink failover feature. If the external network interface of the primary CMM fails, this feature forces a failover to the standby CMM, if one is installed.

**Note:** If a Lenovo Flex System chassis is set up for redundant CMM operation and both CMMs experience an unrecoverable failure, the chassis will attempt to switch control between the CMMs indefinitely. If this condition occurs, replace one CMM to return the chassis to operation or replace both CMMs to return the chassis to redundant operation. Depending on how each CMM failed, you might need to configure the replacement CMM or restore its configuration from a backup, if one is available. A failure of both CMMs might be an indication of other problems with the Lenovo Flex System chassis; make sure that the chassis is operating properly before replacing either CMM. See Troubleshooting chassis for information about diagnosing problems with a Lenovo Flex System chassis.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See “Common errors” on page 407 for a list of error messages that apply to all commands or “uplink command errors” on page 476 for a list of error messages that are specific to the uplink command.

Table 81. uplink command

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display uplink failover status** | Displays the CMM uplink failover status (enabled or disabled) and the failover delay. | `uplink` | Lenovo Flex System chassis:<br>`system`<br>Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[x]`<br>where *x* is the primary CMM bay number. |
| **Set physical network uplink failover delay** | Sets the amount of time between detection of a CMM physical uplink failure and failover to the standby CMM. | `uplink -dps` *delay*<br>where *delay* is from 10 to 172800 seconds, inclusive. If you enter a value outside this range, an error will be displayed.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system`<br>Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[x]`<br>where *x* is the primary CMM bay number. |
| **Enable / disable physical uplink failover** | Enables or disables failover to the standby CMM if the external physical network interface of the primary CMM fails. | `uplink -ep` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system`<br>Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[x]`<br>where *x* is the primary CMM bay number. |

Table 81. uplink command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set logical network uplink failover delay** | Sets the amount of time between detection of a CMM logical uplink failure and failover to the standby CMM. | `uplink -dls` *delay*<br>where *delay* is from 60 to 172800 seconds, inclusive. If you enter a value outside this range, an error will be displayed.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system`<br>Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Enable / disable logical uplink failover** | Enables or disables failover to the standby CMM if the external logical network interface of the primary CMM fails.<br>Failure is indicated when all of the following conditions occur:<br>• Loss of CMM eth0 input and output packets<br>• Network noise<br>• Failures when pinging the CMM gateway and a designated station<br>You must enter a non-zero IPv4 IP address (`-ip` command option) and a non-zero IPv6 IP address (`-ip6` command option) for a device that the CMM can access to check its logical network link before you can enable logical uplink failover. | `uplink -el` *state*<br>where *state* is `enabled` or `disabled` .<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system`<br>Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 81. uplink command (continued)*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set IP address to check logical network uplink** | Sets the IPv4 IP address of the device that the CMM accesses to check its logical network link. | `uplink -ip` *ip_address*<br>where *ip_address* is a valid IPv4 IP address. You must enter a non-zero IPv4 IP address, in dotted decimal IP address format, before you can enable logical uplink failover.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system`<br>Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set IPv6 IP address to check logical network uplink** | Sets the IPv6 IP address of the device that the CMM accesses to check its logical network link. | `uplink -ip6` *ip_address*<br>where *ip_address* is a valid, non-zero, IPv6 IP address. You must enter a non-zero IPv6 IP address before you can enable logical uplink failover.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system`<br>Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set logical link loss alert and failover policy** | Sets the alert and failover policy for logical link loss to check either the IPv4 IP address, the IPv6 IP address, or both of these IP addresses.<br>**Notes:** The `-alert` command option applies only when:<br>• Both the `-ip` and `-ip6` command options are set.<br>• Both IP addresses are non-zero.<br>• IPv6 is enabled using the `ifconfig` command. | `uplink -alert` *setting*<br>where *setting* is:<br>• `either` to check either the IPv4 IP address or the IPv6 IP address.<br>• `both` to check both the IPv4 IP address and the IPv6 IP address.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration | Lenovo Flex System chassis:<br>`system`<br>Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 81. uplink command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | | See "Commands and user authority" on page 10 for additional information. | |

**Example:** To set the IPv4 IP address of the device that the CMM accesses to check its logical network link to 9.72.220.180 and the IPv6 IP address of this device to 1111::2222, while the primary CMM in bay 2 is set as the persistent command environment, at the `system:mm[2]>` prompt, type

```
uplink -ip 9.72.220.180 -ip6 1111::2222
```

To set the alert and failover policy for logical link loss to check for failures of both the IPv4 IP address and the IPv6 IP address, while the primary CMM in bay 2 is set as the persistent command environment, at the `system:mm[2]>` prompt, type

```
uplink -alert both
```

To enable logical link loss failover to the standby CMM if the external logical network interface of the primary CMM fails, while the primary CMM in bay 2 is set as the persistent command environment, at the `system:mm[2]>` prompt, type

```
uplink -el enabled
```

To display the uplink failover configuration, while the primary CMM in bay 2 is set as the persistent command environment, at the `system:mm[2]>` prompt, type

```
uplink
```

The following example shows the information that is returned from these commands:

```
system:mm[2]> uplink -ip 9.72.220.180 -ip6 1111::2222
OK
system:mm[2]> uplink -alert both
OK
system:mm[2]> uplink -el enabled
OK
system:mm[2]> uplink
Failover on network uplink loss is disabled for physical detection
Uplink delay for physical detection: 60 seconds

Failover on network uplink loss is enabled for logical detection
Uplink delay for logical detection: 1800 seconds
Destination IP for MM to check its logical link: 9.72.220.180
Destination IPv6 IP for MM to check its logical link: 1111::2222
Alert and failover if both IPv4 and IPv6 link checks fail
system:mm[2]>
```

## users command

This command displays and configures user accounts, also called user profiles, of the primary CMM.

**Important:** Users and permission groups for the Lenovo Flex System chassis are controlled by the CMM in each Lenovo Flex System chassis, using the CMM CLI "users command" on page 372 and the "permgroups command" on page 238 or the CMM web interface. If your Lenovo Flex System configuration includes an optional management device, such as the Lenovo XClarity Administrator or Flex System Manager hardware, users and permission groups for each optional management device installation are controlled by the management device software (see http://flexsystem.lenovofiles.com/help/topic/com.lenovo.lxca.doc/aug_ product_page.html for information about using the Lenovo XClarity Administrator or http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.8731.doc/product_page.html for information about user and permission group management using the Flex System Manager).

**Notes:**

- Permission groups are viewed and modified using the "permgroups command" on page 238.
- Users can be backed up as part of the CMM configuration using the "write command" on page 404.
- Users are restored as part of a backed up CMM configuration using the "read command" on page 280.
- When the CMM is set to "Secure" security mode, only secure file transfer methods, such as HTTPS and SFTP, can be used for tasks involving file transfer when the CMM is acting as a server. Unsecure file transfer protocols, such as HTTP, FTP, and TFTP, are disabled when the CMM is acting as a server when the security mode is set to "Secure". Unsecure file transfer protocols remain available for a CMM acting as a client for all commands when the security mode is set to "Secure".
- For information about how to specify a URL for file transfer, see "Specifying a URL for file transfer" on page 29.
- Before you update the firmware for Power Systems compute nodes using an optional management device, make sure that the passwords for the Power Systems compute node accounts on the CMM will not expire before the update is complete. If the passwords expire during a code update, the compute nodes might not reconnect to the management software, and each Power Systems compute node might have to be updated with a new password.
- The user accounts set up in the CMM are used to log in to the service processor interfaces of the compute nodes.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "users command errors" on page 477 for a list of error messages that are specific to the users command.

*Table 82. users (CMM users) command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display all user profiles** | Displays all 84 (maximum) CMM user profiles. Returned user values are:<br>• User name<br>• Permission groups<br>• Current number of active sessions<br>• Maximum sessions allowed<br>• State of account (active or inactive)<br>• Password state (expired or not expired)<br>A list of current user permission groups displays after the list of user profiles. | `users` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Display active users** | Displays all users that are currently logged in to the CMM. Returned values include:<br>• User name<br>• Session ID<br>• Inactive time for each connection<br>• User IP address<br>• Connection type | `users -curr` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Terminate user session** | Terminates the specified user login session.<br>**Note:** The session ID is found by running the `users -curr` command. | `users -ts` *sessionID*<br>where *sessionID* is a number that corresponds to the user session ID.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Display single user profile** | Displays the specified CMM user profile. Returned values are:<br>• Permission groups<br>• Current number of active sessions<br>• Maximum sessions allowed<br>• State of account (active or inactive)<br>• Password state (expired or not expired)<br>**Note:** User names are not case sensitive. | `users -n` *user_name*<br>where *user_name* is a user name assigned in the "Display all user profiles" list. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 82. users (CMM users) command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Disable user profile** | Disables the specified CMM user profile.<br>**Note:** User names are not case sensitive. | `users -disable -n` *user_name*<br>where *user_name* is a user name assigned in the "Display all user profiles" list.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Enable user profile** | Enables a specified CMM user profile that is disabled.<br>**Note:** User names are not case sensitive. | `users -enable -n` *user_name*<br>where *user_name* is a user name assigned in the "Display all user profiles" list.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Unlock user profile** | Unlocks a specified CMM user profile that is locked.<br>**Note:** User names are not case sensitive. | `users -unlock -n` *user_name*<br>where *user_name* is a user name assigned in the "Display all user profiles" list.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 82. users (CMM users) command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Delete user profile** | Delete the specified CMM user profile.<br>**Note:** User names are not case sensitive. | `users -clear -n` *user_name*<br>where *user_name* is a user name assigned in the "Display all user profiles" list.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Add user** | Create the specified CMM user. The following user-profile fields are required:<br>• -n *user_name*<br>• -p *user_password*<br>• -g *permission_group*<br>• -ms *max_sessions*<br>**Notes:**<br>• User names and group names are not case sensitive.<br>• Passwords are case sensitive. | `users -add -n` *user_name* `-p` *user_password* `-g` *permission_group* `-ms` *max_sessions*<br>where:<br>• *user_name* is an alphanumeric string up to 32 characters in length that can include periods ( . ), underscores ( _ ), and hyphens ( - ). Each of the 84 (maximum) user names must be unique. User names are not case sensitive.<br>• *user_password* is an alphanumeric string between 5 and 32 characters in length that can include special characters and must include at least one alphabetic and one numeric character, but no white space. Passwords are case sensitive.<br>• *permission_group* are one or more of the user permission groups listed in the "Display all user profiles" list, separated by a vertical bar ( \| ). One default permission group (supervisor or | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 82. users (CMM users) command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | | operator), or one or more custom permission groups can be specified. Group names are not case sensitive.<br>• *max-session* is a number from 0 to 20 that sets the maximum number of simultaneous sessions for the user. A value of 0 means that there is no session limit for the user.<br>*(continued on next page)*<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>See "Commands and user authority" on page 10 for additional information. | |
| **Change user password (own password)** | Allows a user to change the user password in their own CMM user profile.<br>**Notes:**<br>• Users can change their own password even if they do not have authority to manage accounts. The -op option is only used when changing your own password.<br>• User names are not case sensitive.<br>• Passwords are case sensitive. | `users -n` *user_name* `-op` *old_password* `-p` *new_password*<br>where:<br>• *user_name* is your own user name assigned in the "Display all user profiles" list.<br>• *old_password* is your current user password. Passwords are case sensitive.<br>• *new_password* is an alphanumeric string between 5 and 32 characters in length that can include special characters and must include at least one alphabetic and one numeric character, but no white space. Passwords are case sensitive. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 82. users (CMM users) command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | | Users who do not have authority to manage accounts can change their own password using the -op option. | |
| **Change user password (other user)** | Forces a password change in the specified CMM user profile.<br>**Notes:**<br>- User names are not case sensitive.<br>- Passwords are case sensitive.<br>- Users can change their own password, even if they do not have authority to manage accounts, by specifying the -op option (see the `users -op` command description for information. | `users -n` *user_name* `-p` *new_password*<br>where:<br>- *user_name* is a user name assigned in the "Display all user profiles" list.<br>- *new_password* is an alphanumeric string between 5 and 32 characters in length that can include special characters and must include at least one alphabetic and one numeric character, but no white space. Passwords are case sensitive.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>- Supervisor<br>- Chassis account management<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 82. users (CMM users) command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set user permission groups** | Sets the user permission groups in the specified CMM user profile.<br>**Note:** User names and group names are not case sensitive. | `users -n` *user_name* `-g` *permission_group*<br>where:<br>• *user_name* is a user name assigned in the "Display all user profiles" list.<br>• *permission_group* are one or more of the user permission groups listed in the "Display all user profiles" list, separated by a vertical bar (\|). One default permission group (supervisor or operator), or one or more custom permission groups can be specified. Group names are not case sensitive.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set maximum number of simultaneous sessions for user** | Sets the maximum number of simultaneous login sessions for the specified user.<br>**Note:** User names are not case sensitive. | `users -n` *user_name*`-ms` *max-session*<br>where:<br>• *user_name* is a user name assigned in the "Display all user profiles" list.<br>• *max-session* is a number from 0 to 20 that sets the maximum number of simultaneous sessions for the user. A value of 0 means that there is no session limit for the user.<br><br>This command can only be run by users who have one or more of the | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 82. users (CMM users) command (continued)

| **Function** | **What it does** | **Command** | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
|  |  | following command authorities:<br>• Supervisor<br>• Chassis account management<br>See "Commands and user authority" on page 10 for additional information. |  |
| **Add SSH public key to user** | Adds an SSH public key to the specified user.<br>The following user-profile fields are required:<br>• -n *user_name*<br>• -kf *key_format*<br>• -key *key* | `users -add -n` *user_name* `-kf` *key_format* `-key "` *key* `"`<br>where:<br>• *user_name* is a user name assigned in the "Display all user profiles" list.<br>• *key_format* is `openssh`<br>• *key* is an SSH public key, up to 6000 characters in length, enclosed in double-quotes.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 82. users (CMM users) command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Remove SSH public key from user** | Removes one or all SSH public keys associated with the specified user. | `users -remove -n` *user_name* `-ki` *key_index*<br>where:<br>- *user_name* is a user name assigned in the "Display all user profiles" list.<br>- *key_index* is<br>  – an integer between 1 and 20 that identifies a key for the specified user.<br>  – `all` to remove all keys associated with the specified user<br>This command can only be run by users who have one or more of the following command authorities:<br>- Supervisor<br>- Chassis account management<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Import (upload) and add new SSH public key** | Import (upload) and add a new SSH public key for user.<br>The upload location of the key file, including IP address and filename, an must be set using the -u command option. | `users -upld -n` *user_name* `-kf` *key_format* `-u` *URL*<br>where:<br>- *user_name* is a user name assigned in the "Display all user profiles" list.<br>- *key_format* is `openssh`<br>- *URL* is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the key file is located.<br>This command can only be run by users who have one or more of the following command authorities:<br>- Supervisor<br>- Chassis account management<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 82. users (CMM users) command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Import (upload) and update existing SSH public key** | Import (upload) and update existing SSH public key for user.<br>The upload location of the key file, including IP address and filename, an must be set using the -u command option. | `users -upld -n` *user_name* `-ki` *key_index* `-kf` *key_ format* `-u` *URL*<br>where:<br>• *user_name* is a user name assigned in the "Display all user profiles" list.<br>• *key_index* is an integer between 1 and 20 that identifies a key for the specified user.<br>• *key_format* is `openssh`<br>• *URL* is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the key file is located.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Export (download) SSH public key** | Export (download) the specified SSH public key.<br>The download location of the key file, including IP address and filename, and must be set using the -u command option. | `users -dnld -n` *user_name* `-ki` *key_index* `-kf` *key_ format* `-u` *URL*<br>where:<br>• *user_name* is a user name assigned in the "Display all user profiles" list.<br>• *key_index* is an integer between 1 and 20 that identifies a key for the specified user.<br>• *key_format* is `openssh`<br>• *URL* is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the key file is located. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 82. users (CMM users) command (continued)

| Function | What it does | Command | Target (see paths in "Command targets" on page 6) |
|---|---|---|---|
| **Display SSH public key information (summary)** | Displays SSH public key information summary for the specified user. | `users -u` *user_name* `-ki` *key_index*<br>where:<br>• *user_name* is a user name assigned in the "Display all user profiles" list.<br>• *key_index* is<br>– an integer between 1 and 20 that identifies a key for the specified user.<br>– `all` to display all keys associated with the specified user | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Display complete SSH public key information** | Displays complete SSH public key information for the specified user.<br>**Note:** When displaying complete key information, you can only specify one key index each time you run the command. | `users -u` *user_name* `-ki` *key_index* `-kf` *key_format* `-e`<br>where:<br>• *user_name* is a user name assigned in the "Display all user profiles" list.<br>• *key_index* is<br>– an integer between 1 and 20 that identifies a key for the specified user.<br>• *key_format* is `openssh` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 82. users (CMM users) command (continued)*

| **Function** | **What it does** | **Command** | **Target** *(see paths in "*Command targets*" on page 6)* |
|---|---|---|---|
| **Update SSH public key** | Updates the information for the specified SSH public key for the specified user. Information that can be updated includes:<br>• The list of hosts from which the specified user will accept connections.<br>• Comments. | `users -n` *user_name* `-ki` *key_index* `-kf` *key_format* `-key` " *key*" `-af` " *host_list*" `-cm` " *comment*"<br>where:<br>• *user_name* is a user name assigned in the "Display all user profiles" list.<br>• *key_index* is an integer between 1 and 20 that identifies a key for the specified user.<br>• *key_format* is `openssh`<br>• *key* is an SSH public key, up to 6000 characters in length, enclosed in double-quotes.<br>• *host_list* a list of hosts that the specified user will accept connections from, in the format: `from="`*list*`"` where *list* is a comma-separated list, enclosed in double-quotes, of hostnames and IP addresses. The list is limited to 511 characters, with valid characters including: letters, numbers, commas ( , ), asterisks ( * ), question marks ( ? ), exclamation points ( ! ), periods ( . ), hyphens ( - ), colon ( : ), and percent signs ( % ).<br>• *comment* is a string of up to 255 characters in length, enclosed in double-quotes.<br><br>*(continued on next page)* | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Update SSH public key** *(continued)* | | This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>See "Commands and user authority" on page 10 for | |

Table 82. users (CMM users) command (continued)

| Function | What it does | Command | **Target** *(see paths in* "Command targets" *on page 6)* |
|---|---|---|---|
| | | additional information. | |
| **Update user SNMPv3 information** | Updates the SNMPv3 information for the specified user. Information that can be updated includes:<br>• Context name<br>• Authentication protocol<br>• Privacy protocol<br>• Privacy password<br>• Access type<br>• IP address of the SNMPv3 server<br>**Note:** SNMPv3 related command options can also be modified singly for each specified user. | `users -n` *user_name* `-cn` "*context_name*" `-ap` *authentication_protocol* `-pp` *privacy_proto* `-ppw` *privacy_pwd* `-at` *access_type* `-i` *hostname/ip_address*<br>where:<br>• *user_name* is a user name assigned in the "Display all user profiles" list.<br>• *context_name* is a unique string up to 32 characters in length, enclosed in double-quotes.<br>• *authentication_protocol* is `md5` or `sha` .<br>• *privacy_proto* is `des` , `aes` , or `none` .<br>• *privacy_pwd* is an alphanumeric string between 5 and 32 characters in length that can include special characters and must include at least one alphabetic and one numeric character, but no white space. The *privacy_pwd* can be cleared by setting its value to null.<br>• *access_type* is `get` , `set` , or `trap` .<br>• *hostname/ip_address* is the host name or IP address of the SNMPv3 server. The *hostname/ip_address* can be cleared by setting its value to null.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>See "Commands and user authority" on page 10 for | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 82. users (CMM users) command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| | | additional information. | |
| **Enable / disable compute node and I/O module account management by CMM** | Enables management by CMM of the IPMI and SNMPv3 user accounts for compute nodes and of the SNMPv3 user accounts for I/O Modules.<br>This command option allows the CMM user accounts to be used for managing most compute nodes and I/O modules in the chassis instead of having management device user accounts manage the compute nodes and the I/O modules.<br>**Important:** Management of compute node IPMI and SNMPv3 user accounts is not supported by POWER-based compute nodes and by I/O modules with firmware versions lower than 8.4.3.<br>**Notes:**<br>• Enabling CMM management of IPMI/SNMPv3 user accounts on nodes causes all existing IPMI/SNMPv3 user accounts on compute nodes to be overwritten. Save existing compute node IPMI/SNMPv3 user account information before enabling compute node account management by the CMM.<br>• Enabling CMM management of SNMPv3 user accounts on I/O modules disables the local SNMPv3 user accounts on I/O modules until the account management by CMM is disabled. | `users -am` *state* `-prov_target` *target*<br>where:<br>• *state* is enabled or disabled.<br>• *target* is "iom", "node" or "all" and it specifies the devices for which the account management should be enabled/disabled: "node": compute nodes, "iom": I/O modules and "all": both compute nodes and I/O modules.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 82. users (CMM users) command (continued)*

| Function | What it does | Command | **Target** *(see paths in "*Command targets*" on page 6)* |
|---|---|---|---|
| **Enable / disable SNMPv3 and/or IPMI centralized management** | Enables or disables centralized management of SNMPv3 and/or IPMI user accounts, including user provisioning.<br>This command enables you to control whether or not specific CMM user accounts can be used to manage chassis components (including provisioning). There can be up to 12 provisioned user accounts for nodes and up to 12 provisioned user accounts for I/O modules. Remember that enabling a user account will not actually allow local management of chassis components unless you have enabled compute node and/or I/O module account management by CMM using the `users -am enabled` command option.<br>**Note:** Disabling centralized IPMI and SNMPv3 management (provisioning) of a user account deletes the centrally managed user account. If there is a corresponding local account for this user on the CMM, it will remain functional. | `users -ipmisnmpv3` *state* `-n` *user_name* `-prov_target` *target*<br>where:<br>• *state* is `enabled` or `disabled` .<br>• *user_name* is a user name assigned in the "Display all user profiles" list.<br>• *target* is "iom", "node" or "all" and it specifies the devices for which the account management should be enabled/disabled: "node": compute nodes, "iom": I/O modules and "all": both compute nodes and I/O modules.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis account management<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Change new user creation method** | Changes new user creation method. There are two available:<br>• username&password" (default)<br>• username&email<br>See "User Authority Management" in *Lenovo Chassis Management Module 2 User's Guide* for more information.<br>**Note:** An email server must be configured in network settings before"username&email" method can be selected (see "CMM management options" in *Lenovo Chassis Management Module 2 User's Guide*). | `users -nucm` *state*<br>where *state* is `username&password` or `username&email`: | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

**Example:** To create a user with a user name of user3, with a password of passw0rd, who is a member of the super permission group (supervisor rights to all Lenovo Flex System components, as defined by the “permgroups command” on page 238), and a maximum number of user sessions of 10, while the primary CMM in bay 2 is set as the persistent command environment, at the system:mm[2]> prompt, type

```
users -add -n user3 -p passw0rd -g super -ms 10
```

To display all users, while the primary CMM in bay 2 is set as the persistent command environment, at the system:mm[2]> prompt, type

```
users
```

To display information for the user named test, while the primary CMM in bay 2 is set as the persistent command environment, at the system:mm[2]> prompt, type

```
users -n test
```

To add a public key of the type openssh to the user named test, with a key value of ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAvfnTUzRF7pdBuaBy4dO/ aIFasa/Gtc+o/ wIZnuC4aDHMA1UmnMyLOCiIaNOy4OOICEKCqjKEhrYymtAo VtfKApvY39GpnSGRC/ qcLGWLM4cmirKL5kxHNOqIcwbT1NPceoKHj46X7E+ mqIfWnAhhjDpcVFjagM3Ek2y7w/ tBGrwGgN7DPHJU1tzcJy68mEAnIrzjUoR98Q3/ B9cJD77ydGKe8rPdI2hIEpXR5dNUiupA1Yd8PSSMgdukASKEd3eRRZTBI3SAt MucUsTkYjIXcqex1OQz4 +N50R6MbNcwIsx+mTEAvvcpJhuga70UNPGhLJMI6k7 jeJiQ8Xd2pXbOZQ==, while the primary CMM in bay 2 is set as the persistent command environment, at the system:mm[2]> prompt, type

```
users -n test -add -kf openssh -key "ssh-rsa AAAAB3NzaC1yc2EAAAA
BIwAAAQEAvfnTUzRF7pdBuaBy4dO/aIFasa/Gtc+o/wlZnuC4aDHMA1UmnMyLOCiIaNOy4OOICEKCq
jKEhrYymtAoVtfKApvY39GpnSGRC/qcLGWLM4cmirKL5kxHNOqIcwbT1NPceoKHj46X7E+mqlfWnAh
hjDpcVFjagM3Ek2y7w/tBGrwGgN7DPHJU1tzcJy68mEAnIrzjUoR98Q3/B9cJD77ydGKe8rPdI2hIE
pXR5dNUiupA1Yd8PSSMgdukASKEd3eRRZTBl3SAtMucUsTkYjlXcqex1OQz4+N50R6MbNcwlsx+mTE
AvvcpJhuga70UNPGhLJMl6k7jeJiQ8Xd2pXbOZQ=="
```

To display the key with an index of 1 for the user named test, while the primary CMM in bay 2 is set as the persistent command environment, at the system:mm[2]> prompt, type

```
users -n test -ki 1
```

To display all keys for the user named test, while the primary CMM in bay 2 is set as the persistent command environment, at the system:mm[2]> prompt, type

```
users -n test -ki all
```

To display full key information for the key with an index of 1, of type openssh, for the user named test, while the primary CMM in bay 2 is set as the persistent command environment, at the system:mm[2]> prompt, type

```
users -n test -ki 1 -kf openssh -e
```

To download a key with an index of 1, of type openssh, for the user named test, from tftp://9.72.216.40/file.key, while the primary CMM in bay 2 is set as the persistent command environment, at the system:mm[2]> prompt, type

```
users -n test -dnld -ki 1 -kf openssh -u tftp://9.72.216.40/file.key
```

To upload a key with an index of 1, of type openssh, for the user named test, from tftp://9.72.216.40/file.key, while the primary CMM in bay 2 is set as the persistent command environment, at the system:mm[2]> prompt, type

```
users -n test -upld -ki 1 -kf openssh -u tftp://9.72.216.40/file.key
```

To remove a key with an index of 1 for the user named test, while the primary CMM in bay 2 is set as the persistent command environment, at the system:mm[2]> prompt, type

```
users -n test -ki 1 -remove
```

To remove all keys for the user named test, while the primary CMM in bay 2 is set as the persistent command environment, at the system:mm[2]> prompt, type

```
users -n test -ki all -remove
```

The following example shows the information that is returned from these commands:

```
system:mm[2]> users -add -n user3 -p passw0rd -g super -ms 10
OK
system:mm[2]> users

Node provisioning: disabled
I/O module provisioning: disabled

Users
=====

USERID
   Group(s): supervisor
   1 active session(s)
   Max 0 session(s) allowed
   Account is active
   Password is not expired
   Password is compliant
   There is no SSH public key installed for this user
   IPMI and SNMPv3 user provisioning for nodes is disabled
   SNMPv3 user provisioning for I/O modules is disabled

user3
   Group(s): super
   0 active session(s)
   Max 10 session(s) allowed
   Account is active
   Password is not expired
   Password is compliant
   There is no SSH public key installed for this user
   IPMI and SNMPv3 user provisioning for nodes is disabled
   SNMPv3 user provisioning for I/O modules is disabled

test
   Group(s): opmin
   0 active session(s)
   Max 2 session(s) allowed
   Account is active
   Password is not expired
   Password is compliant
   Number of SSH public keys installed for this user: 2
   IPMI and SNMPv3 user provisioning for nodes is disabled
   SNMPv3 user provisioning for I/O modules is disabled

User Permission Groups
======================

supervisor
   Role:supervisor
   Blades:1|2|3|4|5|6|7|8|9|10|11|12|13|14
   Chassis:1
   Modules:1|2|3|4|5|6|7|8|9|10

operator
   Role:operator
   Blades:1|2|3|4|5|6|7|8|9|10|11|12|13|14
   Chassis:1
   Modules:1|2|3|4|5|6|7|8|9|10

opmin
```

```
   Role:operator
   Blades:n/a
   Chassis:n/a
   Modules:n/a


system:mm[2]> users -n test

-g opmin
-ms 5
-cn admin
-ap sha
-pp des
-at set
-i 0.0.0.0
Node provisioning: -ipmisnmpv3 disabled
I/O module provisioning: -snmpv3 disabled
0 active session(s)
Max 2 session(s) allowed
Account is active
Password is not expired
Password is compliant
Number of SSH public keys installed for this user: 2
Last login: Never


system:mm[2]> users -n test -add -kf openssh -key "ssh-rsa AAAAB3NzaC1yc2EAAAA
BIwAAAQEAvfnTUzRF7pdBuaBy4dO/aIFasa/Gtc+o/wlZnuC4aDHMA1UmnMyLOCiIaNOy4OOICEKCq
jKEhrYymtAoVtfKApvY39GpnSGRC/qcLGWLM4cmirKL5kxHNOqIcwbT1NPceoKHj46X7E+mqlfWnAh
hjDpcVFjagM3Ek2y7w/tBGrwGgN7DPHJU1tzcJy68mEAnIrzjUoR98Q3/B9cJD77ydGKe8rPdI2hIE
pXR5dNUiupA1Yd8PSSMgdukASKEd3eRRZTBl3SAtMucUsTkYjlXcqex1OQz4+N5OR6MbNcwlsx+mTE
AvvcpJhuga7OUNPGhLJMl6k7jeJiQ8Xd2pXbOZQ=="
OK


system:mm[2]> users -n test
-g opmin
-ms 5
-cn admin
-ap sha
-pp des
-at set
-i 0.0.0.0
Node provisioning: -ipmisnmpv3 disabled
I/O module provisioning: -snmpv3 disabled
0 active session(s)
Max 2 session(s) allowed
Account is active
Password is not expired
Password is compliant
Number of SSH public keys installed for this user: 3
Last login: Never


system:mm[2]> users -n test -ki 1
ssh-rsa 2048 bits 69:d0:2d:4e:72:09:88:0d:ff:63:87:2c:26:5d:f6:f2
-af
-cm
system:mm[2]> users -n test -ki all

Key 1
```

```
ssh-rsa 2048 bits 69:d0:2d:4e:72:09:88:0d:ff:63:87:2c:26:5d:f6:f2
-af
-cm

Key 2
ssh-rsa 2048 bits 69:d0:2d:4e:72:09:88:0d:ff:63:87:2c:26:5d:f6:f2
-af
-cm

Key 3
ssh-rsa 2048 bits 69:d0:2d:4e:72:09:88:0d:ff:63:87:2c:26:5d:f6:f2
-af
-cm


system:mm[2]> users -n test -ki 1 -kf openssh -e
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAvfnTUzRF7pdBuaBy4dO/aIFasa/Gtc+o/wlZnuC4aD
HMA1UmnMyLOCiIaNOy4OOICEKCqjKEhrYymtAoVtfKApvY39GpnSGRC/qcLGWLM4cmirKL5kxHNOqI
cwbT1NPceoKHj46X7E+mqlfWnAhhjDpcVFjagM3Ek2y7w/tBGrwGgN7DPHJU1tzcJy68mEAnIrzjUo
R98Q3/B9cJD77ydGKe8rPdI2hIEpXR5dNUiupA1Yd8PSSMgdukASKEd3eRRZTBl3SAtMucUsTkYjlX
cqex1OQz4+N5OR6MbNcwlsx+mTEAvvcpJhuga7OUNPGhLJMl6k7jeJiQ8Xd2pXbOZQ==


system:mm[2]> users -n test -dnld -ki 1 -kf openssh -u tftp://9.72.216.40/file.key
OK


system:mm[2]> users -n test -upld -ki 1 -kf openssh -u tftp://9.72.216.40/file.key
OK


system:mm[2]> users -n test -ki 1 -remove
OK


system:mm[2]> users -n test -ki all -remove
OK
```

## vlan command

This command configures and displays the VLAN (virtual local area network) settings for the CMM.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See “Common errors” on page 407 for a list of error messages that apply to all commands or “vlan command errors” on page 481 for a list of error messages that are specific to the vlan command.

**Note:** When viewing the vlan entries, settings preceded by an option (for example, `-i`) can be modified and settings preceded by a label (for example, `IPv4 address:`) are fixed.

*Table 83. vlan command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display all VLAN settings** | Displays all VLAN settings for specified command target.<br>**Note:** The command issued by itself will display all entries, the global state, the commit timeout, and whether the current configuration has been committed. | `vlan` | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Display VLAN settings for specific VLAN ID** | Displays VLAN settings for the specified VLAN ID of the command target. | `vlan -vi` *index*<br>where *index* is the VLAN entry index number. | Lenovo Flex System chassis:<br>`system`<br>Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Apply CMM VLAN settings** | Applies changes made to the CMM VLAN configuration.<br>**Note:** You must commit CMM VLAN configuration changes before the commit timeout expires or the previous configuration is restored. | `vlan -commit`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **CMM commit timeout** | Sets a custom timeout value for applying CMM VLAN configuration changes. If CMM VLAN configuration changes are not committed before the commit timeout expires, the previous configuration is restored. | `vlan -cto` *timeout*<br>where *timeout* is from 1 to 255 minutes, inclusive.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 83. vlan command (continued)

| Function | What it does | Command | Target *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set global VLAN state** | Enables or disables the global VLAN state.<br>**Notes:**<br>• The value of the global VLAN state does not change individual VLAN settings.<br>• All changes to the CMM configuration must be applied using the `vlan -commit` command option, before the commit timeout expires. | `vlan -state` *state*<br>where *state* is<br>• enabled<br>• disabled<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set VLAN state for non-fixed entry** | Sets the VLAN state of the specified non-fixed entry.<br>**Note:** All changes to the CMM configuration must be applied using the `vlan -commit` command option, before the commit timeout expires. | `vlan -vi` *index* `-state` *state*<br>where<br>• *index* is the VLAN entry index number.<br>• *state* is<br>– enabled<br>– disabled<br>– restart<br>This command can only be run by users who have one or more of the following command authorities.<br>• For the Lenovo Flex System chassis target:<br>– Supervisor<br>– Blade configuration<br>• For the primary CMM target:<br>– Supervisor<br>– Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system`<br>Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 83. vlan command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Delete all non-fixed VLAN entries** | Deletes all non-fixed VLAN entries.<br>**Note:** All changes to the CMM configuration must be applied using the `vlan -commit` command option, before the commit timeout expires. | `vlan -delete`<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Delete specific VLAN entry** | Deletes the specified VLAN entry.<br>**Note:** All changes to the CMM configuration must be applied using the `vlan -commit` command option, before the commit timeout expires. | `vlan -vi` *index*`-delete`<br>where *index* is the VLAN entry index number.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Create VLAN entry** | Creates the specified VLAN entry.<br>**Notes:**<br>• `-vi` and `-vid` must both be set to create an entry.<br>• The `-state` and `-n` (name) are set as optional parameters.<br>• A default entry name is used if `-n` is not specified.<br>• All changes to the CMM configuration must be applied using the `vlan -commit` command option, before the commit timeout expires. | `vlan -vi` *index*`-vid` *vlan_id*<br>where<br>• *index* is an unused VLAN entry index number.<br>• *vlan_id* is the number from 1 to 4,094, inclusive.<br>This command can only be run by users who have one or more of the following command authorities.<br>• For the Lenovo Flex System chassis target:<br>– Supervisor<br>– Blade configuration<br>• For the primary CMM target:<br>– Supervisor<br>– Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system`<br>Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 83. vlan command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set VLAN ID** | Sets a new ID for the specified VLAN entry.<br>**Note:** All changes to the CMM configuration must be applied using the `vlan -commit` command option, before the commit timeout expires. | `vlan -vi` *index* `-vid` *id*<br>where<br>• *index* is the VLAN entry index number.<br>• *id* is the number from 1 to 4,094, inclusive.<br>This command can only be run by users who have one or more of the following command authorities.<br>• For the Lenovo Flex System chassis target:<br>– Supervisor<br>– Blade configuration<br>• For the primary CMM target:<br>– Supervisor<br>– Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Lenovo Flex System chassis:<br>`system`<br>Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set SOL access state** | Enables or disables SOL access for the specified VLAN entry.<br>**Notes:**<br>• Before enabling SOL access, you must first to disable it on the VLAN where it is enabled.<br>• If only one VLAN is in use, you cannot disable SOL access.<br>• If both VLANs are in use, disabling or enabling SOL access on one VLAN enables or disables -SOL access on the other VLAN, so that SOL is always enabled on at least one VLAN.<br>• All changes to the CMM configuration must be applied using the `vlan -commit` command option, before the commit timeout expires. | `vlan -vi` *index* `-sol` *state*<br>where<br>• *index* is the VLAN entry index number.<br>• *state* is enabled or disabled.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 83. vlan command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set VLAN tagging state (fixed entry)** | Enables or disabled VLAN tagging for the default (fixed) entry.<br>**Note:** All changes to the CMM configuration must be applied using the `vlan -commit` command option, before the commit timeout expires. | `vlan -vi` *index* `-tag` *state*<br>where<br>• *index* is 1 (the fixed VLAN entry index number).<br>• *state* is enabled or disabled.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set VLAN entry name** | Sets a name for the specified VLAN entry.<br>**Note:** All changes to the CMM configuration must be applied using the `vlan -commit` command option, before the commit timeout expires. | `vlan -vi` *index* `-n` *name*<br>where<br>• *index* is the VLAN entry index number.<br>• *name* is the quote-delimited VLAN entry name, of 1 to 31 characters in length.<br>• For the Lenovo Flex System chassis target:<br>– Supervisor<br>– Blade configuration<br>• For the primary CMM target:<br>– Supervisor<br>– Chassis configuration | Lenovo Flex System chassis:<br>`system`<br>Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set VLAN IPv4 configuration method to static** | Sets the IPv4 configuration method for the specified VLAN non-fixed entry to static.<br>**Note:** All changes to the CMM configuration must be applied using the `vlan -commit` command option, before the commit timeout expires. | `vlan -vi` *index* `-c` *method*<br>where<br>• *index* is the VLAN entry index number.<br>• *method* is static.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 83. vlan command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set VLAN IP address (IPv4)** | Sets the IPv4 address for the specified VLAN non-fixed entry.<br>**Note:** All changes to the CMM configuration must be applied using the `vlan -commit` command option, before the commit timeout expires. | `vlan -vi` *index* `-i` *ip_address*<br>where<br>- *index* is the VLAN entry index number.<br>- *ip_address* is a valid IPv4 IP address.<br>This command can only be run by users who have one or more of the following command authorities:<br>- Supervisor<br>- Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set VLAN subnet (IPv4)** | Sets the IPv4 subnet for the specified VLAN non-fixed entry.<br>**Note:** All changes to the CMM configuration must be applied using the `vlan -commit` command option, before the commit timeout expires. | `vlan -vi` *index* `-s` *subnet*<br>where<br>- *index* is the VLAN entry index number.<br>- *subnet* is the IPv4 subnet.<br>This command can only be run by users who have one or more of the following command authorities:<br>- Supervisor<br>- Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set VLAN gateway (IPv4)** | Sets the IPv4 gateway for the specified VLAN non-fixed entry.<br>**Note:** All changes to the CMM configuration must be applied using the `vlan -commit` command option, before the commit timeout expires. | `vlan -vi` *index* `-g` *gateway*<br>where<br>- *index* is the VLAN entry index number.<br>- *gateway* is the IPv4 gateway.<br>This command can only be run by users who have one or more of the following command authorities:<br>- Supervisor<br>- Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 83. vlan command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set VLAN IPv4 subnet route** | Sets a custom value for the specified IPv4 subnet route of the specified VLAN non-fixed entry.<br>**Note:** All changes to the CMM configuration must be applied using the `vlan -commit` command option, before the commit timeout expires. | `vlan -vi` *index* `-sr` *xsubnet_route*<br>where<br>- *index* is the VLAN entry index number.<br>- *x* is the subnet route number 1, 2, or 3.<br>- *subnet_route* is the IPv4 subnet route.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>- Supervisor<br>- Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set VLAN IPv4 subnet mask** | Sets a custom value for the specified IPv4 subnet mask for the specified VLAN non-fixed entry.<br>**Note:** All changes to the CMM configuration must be applied using the `vlan -commit` command option, before the commit timeout expires. | `vlan -vi` *index* `-sm` *xsubnet_mask*<br>where<br>- *index* is the VLAN entry index number.<br>- *x* is the subnet route number 1, 2, or 3.<br>- *subnet_mask* is the IPv4 subnet mask.<br><br>This command can only be run by users who have one or more of the following command authorities:<br>- Supervisor<br>- Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

Table 83. vlan command (continued)

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set VLAN IPv6 configuration method to static** | Sets the IPv6 configuration method for the specified VLAN non-fixed entry to static. | `vlan -vi` *index* `-c6` *method*<br>where<br>• *index* is the VLAN entry index number.<br>• *method* is static.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set VLAN IP address (IPv6)** | Sets the IPv6 address for the specified VLAN non-fixed entry.<br>**Note:** All changes to the CMM configuration must be applied using the `vlan -commit` command option, before the commit timeout expires. | `vlan -vi` *index* `-i6` *ip_address*<br>where<br>• *index* is the VLAN entry index number.<br>• *ip_address* is a valid IPv6 IP address.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 83. vlan command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set VLAN IPv6 prefix length** | Sets the IPv6 prefix length for the specified VLAN non-fixed entry.<br>**Note:** All changes to the CMM configuration must be applied using the `vlan -commit` command option, before the commit timeout expires. | `vlan -vi` *index* `-p6` *prefix_length*<br>where<br>• *index* is the VLAN entry index number.<br>• *prefix_length* is the IPv6 prefix length, between 1 and 128 (inclusive).<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set VLAN gateway (IPv6)** | Sets the IPv6 gateway for the specified VLAN non-fixed entry.<br>**Note:** All changes to the CMM configuration must be applied using the `vlan -commit` command option, before the commit timeout expires. | `vlan -vi` *index* `-g6` *gateway*<br>where<br>• *index* is the VLAN entry index number.<br>• *gateway* is the IPv6 gateway.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

*Table 83. vlan command (continued)*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Set VLAN IPv6 subnet route** | Sets a custom value for the specified IPv6 subnet route of the specified VLAN non-fixed entry.<br>**Note:** All changes to the CMM configuration must be applied using the `vlan -commit` command option, before the commit timeout expires. | `vlan -vi` *index* `-sr6`*x* *subnet_route*<br>where<br>• *index* is the VLAN entry index number.<br>• *x* is the subnet route number 1, 2, or 3.<br>• *subnet_route* is the IPv6 subnet route.<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |
| **Set VLAN IPv6 subnet prefix length** | Sets a custom value for the specified IPv6 subnet prefix length for the specified VLAN non-fixed entry.<br>**Note:** All changes to the CMM configuration must be applied using the `vlan -commit` command option, before the commit timeout expires. | `vlan -vi` *index* `-sp6`*x* *prefix_length*<br>where<br>• *index* is the VLAN entry index number.<br>• *x* is the subnet route number 1, 2, or 3.<br>• *prefix_length* is the IPv6 subnet prefix length, between 1 and 128 (inclusive).<br>This command can only be run by users who have one or more of the following command authorities:<br>• Supervisor<br>• Chassis configuration<br>See "Commands and user authority" on page 10 for additional information. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

**Example:**

To display all VLAN settings, while the CMM in bay 2 is set as the persistent command environment, at the `system:mm[2]>` prompt, type

```
vlan
```

To disable the global VLAN state, while the CMM in bay 2 is set as the persistent command environment, at the `system:mm[2]>` prompt, type

```
vlan -state disabled
```

To delete the VLAN entry with an index number of 2, while the CMM in bay 2 is set as the persistent command environment, at the `system:mm[2]>` prompt, type

```
vlan -delete -vi 2
```

To apply (commit) all changes made to VLAN settings, while the CMM in bay 2 is set as the persistent command environment, at the `system:mm[2]>` prompt, type

```
vlan -commit
```

To display the VLAN settings for the compute node with a VLAN ID of 1, while the CMM in bay 2 is set as the persistent command environment, at the `system:mm[2]>` prompt, type

```
vlan -vi 1
```

The following example shows the information that is returned from these commands:

```
view all CMM VLAN entries:

system:mm[2]> vlan
-state enabled
-cto 2

-vi 1
-n VLAN-1
-state enabled
-vid 1
-sol enabled
-tag disabled
IPv4 config method: static
IPv4 address: 9.37.64.201
IPv4 subnet: 255.255.252.0
IPv4 gateway: 9.37.64.1
IPv6 config method: static
IPv6 address: ::
IPv6 prefix length: 0
IPv6 gateway: ::

-vi 2
-n temp vlan
-state disabled
-vid 2000
-sol disabled
-c static
-i 192.168.70.125
-s 255.255.255.255
-g 0.0.0.0
-sr1 0.0.0.0
-sm1 255.255.255.255
-sr2 0.0.0.0
-sm2 255.255.255.255
-sr3 0.0.0.0
-sm3 255.255.255.255
-c6 static
-i6 1122::3344
-p6 0
-g6 ::
-sr61 ::
-sp61 0
-sr62 ::
-sp62 0
```

```
-sr63 ::
-sp63 0

The current configuration has been committed.
system:mm[2]> vlan -state disabled
All changes must be committed using -commit before the commit timeout expires.
OK
system:mm[2]> vlan -delete -vi 2
All changes must be committed within 20 minutes using -commit.
OK
system:mm[2]> vlan -commit
OK
system:mm[2]> vlan -vi 1
-vi 1
-n VLAN-1
-state disabled
-vid 10
system:mm[2]
```

## volts command

This command displays actual voltages and voltage threshold values for Lenovo Flex System components.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See "Common errors" on page 407 for a list of error messages that apply to all commands or "volts command errors" on page 484 for a list of error messages that are specific to the volts command.

*Table 84. volts command*

| Function | What it does | Command | **Target** *(see paths in "Command targets" on page 6)* |
|---|---|---|---|
| **Display voltage values** | Displays the current voltage and voltage threshold settings for the specified compute node.<br>**Note:** The voltage values that display will vary based on chassis and compute node type. | `volts` | Compute node:<br>`blade[x]`<br>where *x* is the node bay number. |

**Example:** To view the current voltage and voltage thresholds for the first compute node in the storage expansion enclosure in bay 11, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type
`volts -T bladeenclosure[11]:blade[1]`

The following example shows the information that is returned from this command:

```
system> volts -T bladeenclosure[11]:blade[1]
    Source         Value      Critical
---------------   -------   ----------------
Planar 3.3V      +3.35    (+2.96,+3.62)
Planar 5V         +5.10    (+4.48,+5.49)
Planar 12V        +12.37   (+10.78,+13.20)
Planar VBAT       +2.92    (+2.70,+3.18)
system>
```

## write command

This command saves the CMM configuration, including user accounts and permission groups, to a file.

Saved configurations are restored using the “read command” on page 280.

**Notes:**

- When the CMM is set to “Secure” security mode, only secure file transfer methods, such as HTTPS and SFTP, can be used for tasks involving file transfer when the CMM is acting as a server. Unsecure file transfer protocols, such as HTTP, FTP, and TFTP, are disabled when the CMM is acting as a server when the security mode is set to “Secure”. Unsecure file transfer protocols remain available for a CMM acting as a client for all commands when the security mode is set to “Secure”.
- For information about how to specify a URL for file transfer, see “Specifying a URL for file transfer” on page 29.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See “Common errors” on page 407 for a list of error messages that apply to all commands or “write command errors” on page 484 for a list of error messages that are specific to the write command.

*Table 85. write command*

| Function | What it does | Command | **Target** *(see paths in “*Command targets*” on page 6)* |
|---|---|---|---|
| **Save CMM configuration to file** | Saves an image of the CMM configuration to a file. This image includes CMM users and permission groups. | `write -u` *URL* `-p` *passphrase*<br>where:<br>• *URL* is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the configuration file will be saved.<br>• "*passphrase*" is a double-quote delimited passphrase that will be needed to restore the configuration file. Minimum passphrase length is 6 characters. Maximum passphrase length is 31 characters. | Primary CMM:<br>`mm[p]`<br>`mm[P]`<br>`mm[`*x*`]`<br>where *x* is the primary CMM bay number. |

**Example:**

To save the CMM configuration to a file named cmm1.cfg in the temp directory on a TFTP server with an IP address of 9.37.177.215 and a passphrase of backuplock, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
write -u tftp://9.37.177.215/temp/cmm1.cfg -p "backuplock" -T mm[p]
```

The following example shows the information that is returned from this command:

```
system> write -u tftp://9.37.177.215/temp/cmm1.cfg -p "backuplock" -T mm[p]
```

```
OK
```

To save the CMM configuration to a file named cfg.bkp in the /tftpboot/backup directory on a SFTP server with an IP address of 300.370.640.310, a user ID of userid, and a passphrase of Passphaase, while the Lenovo Flex System chassis is set as the persistent command environment, at the `system>` prompt, type

```
write -T mm[p] -p "Passphaase" -u sftp://userid:password@300.370.640.310/tftpboot/
backup/cfg.bkp
```

The following example shows the information that is returned from this command:

```
system> write -T mm[p] -p "Passphaase" -u sftp://userid:password@300.370.640.310/
tftpboot/backup/cfg.bkp
OK
```

# Chapter 4. Error messages

The Lenovo Flex SystemChassis Management Module 2 command-line interface provides both common error messages that apply to all commands and command-specific error messages.

The following topics list error messages and their definitions. Common messages appear first, with error messages for each command following in alphabetic order.

## Common errors

This topic lists error messages that apply to all commands.

Each command that has unique errors will also have a list of command-specific error messages.

*Table 86. Common errors*

| Error message | Definition |
|---|---|
| Command cannot be issued to this target. Type env -h for help on changing targets. | A user tries to issue a command to a target that does not support that command. |
| Command line contains extraneous arguments. | A user tries to enter a command with extra command arguments. |
| Duplicate option: *option*<br>where *option* identifies the command option that was entered more than once. | A user tries to enter the same command option in a single command multiple times. For example, `dns -i 192.168.70.29 -i` |
| Each option can only be used once per command. | A user tries to enter the same command option in a single command multiple times. For example, `env -T system:blade [4] -T system:blade[5]`. |
| Error: Command not recognized. Type 'help' to get a list of supported commands. | A user tries to enter a command that does not exist. |
| Error creating data buffer for read | An error occurs while creating a read data buffer. |
| Error creating data buffer for write | An error occurs while creating a write data buffer. |
| Error parsing data | There is an error in the data that was received. |
| Error reading data for the option - *option*<br>where *option* identifies the command option that is returning an error. | An error occurs while the CMM is reading data of a option. |
| Error writing data for the option *option*<br>where *option* identifies the command option that is returning an error. | An error occurs while the CMM is writing a command option value. |
| Firmware update is in progress. Try again later. | Firmware update is in progress. |
| Illegal option *option* for the target.<br>where *option* identifies the option that is invalid. | A user tries to issue a command with an invalid option for the target. |
| Illegal option: *option*<br>where *option* identifies the illegal short command option that was entered. | A user tries to enter an illegal short command option. |

Table 86. Common errors (continued)

| Error message | Definition |
|---|---|
| Integer argument out of range (*range* - *range*) for -*option*: *argument*<br>where:<br>• *range* identifies the range limits<br>• *option* identifies the command option<br>• *argument* identifies the integer that is out of range | A user tries to enter an integer argument that is out of range. |
| Internal error. | An internal error occurs. |
| Invalid integer argument for -*option*: *argument*<br>where:<br>• *option* identifies the command option<br>• *argument* identifies the invalid argument | A user tries to enter an invalid integer argument for the specified command option. |
| Invalid option. | A user tries to enter an invalid command option. |
| Invalid option argument for *option*: *argument*<br>where:<br>• *option* identifies the command option<br>• *argument* identifies the invalid argument | A user tries to enter an invalid argument for the specified command option. |
| Invalid option argument for *option*: arguments containing spaces must be enclosed in quotation marks.<br>where *option* identifies the command option | A user tries to enter an argument containing spaces for the specified command option, without enclosing the argument in double-quotation marks. |
| Invalid option for this target: *option*<br>where *option* identifies the option that is invalid. | A user tries to issue a command with an invalid option for the target. |
| Invalid parameter. Input must be numeric. | A user tries to enter a non-numeric argument. |
| Invalid syntax. Type *command* - h for help.<br>where *command* identifies the command that is returning an error. | A user tries to enter a command that is not syntactically correct. |
| Invalid target path. | A user tries to issue a command to a target that is not valid. |
| Long option *option* requires an argument<br>where *option* identifies the short command option that is missing an argument. | A user tries to enter a long command option without a required argument. |
| Missing option name | A user tries to enter a dash (-) without a command option name. |
| Option argument for *option* exceeds max length (*max* characters): *argument*<br>where:<br>• *option* identifies the option that has an argument of excessive length.<br>• *max* is the maximum allowed argument length.<br>• *argument* is the argument that was entered. | A user tried to enter an option argument that exceeds the maximum allowed length. |
| Read/write command error. | An error occurs while the CMM is executing the command. |
| Short option *option* requires an argument<br>where *option* identifies the short command option that is missing an argument. | A short command option is entered without a required argument. |
| Syntax error. Type *command* -h for help.<br>where *command* identifies the command that is returning an error. | A user tries to enter a command improperly. |

Table 86. Common errors (continued)

| Error message | Definition |
|---|---|
| The argument for option *option* is outside the valid range.<br>where *option* identifies the command option that has an out of range argument. | A user tries to enter an argument that is outside of the valid range for the option. |
| The argument for option *option* is outside the valid range of *minimum* - *maximum*<br>where:<br>• *option* identifies the command option that has an out of range argument.<br>• *minimum* is the smallest allowed value<br>• *maximum* is the largest allowed value | A user tries to enter an argument that is outside of the valid range for the option. |
| The argument for option *option* must be numeric.<br>where *option* identifies the command option that has a non-numeric argument. | A user tries to enter an argument that is not numeric, when the option requires a numeric argument. |
| The target bay is empty. | A user tries to issue a command to an empty compute node bay, fan module bay, I/O bay, CMM bay, or power bay. |
| The target bay is out of range. | A user tries to issue a command to a target that is out of range for that target. For example, the `env -T system:blade[15]` command is out of range because the Lenovo Flex System chassis has only 14 node bays. |
| The target slot is out of range. | A user tries to issue a command to a target which is out of range for that target. |
| There was a problem retrieving the file. | An error occurred when transferring the file. |
| Unable to validate target. | An error occurred when validating a command target. |
| Unable to verify target presence. | An error occurred when verifying that a command target is present. |
| Unknown long option: *option*<br>where *option* identifies the command option that is unknown. | A user tries to enter a long option that is not valid for the command. |
| Unknown option: *option*<br>where *option* identifies the command option that is unknown. | A user tries to enter an unknown command option. |
| Unrecognized long option: *option*<br>where *option* identifies the illegal long command option that was entered. | A user tries to enter an illegal long command option. |
| Unsupported target type. | A user tries to issue a command to an unsupported target. |
| User does not have the authority to issue this command. | A user lacks the authority level necessary to execute a command. |
| Validating target slot failed | An error occurred when validating the target. |

## accseccfg command errors

This topic lists error messages for the accseccfg command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “accseccfg command” on page 39 for information about command syntax and examples of command use.

Table 87. accseccfg command errors

| Error message | Definition |
|---|---|
| -dc can not be enabled when -rc or/and -cp is/are disabled or being disabled. | A user tries to set a minimum number of different password characters that conflicts with password reuse cycle (-rc) and complex password (-cp) settings. |
| -dc is being disabled as -cp or/and -rc is/are disabled or being disabled. | A user tries to disable the minimum number of different password characters when it conflicts with password reuse cycle (-rc) and complex password (-cp) settings. |
| -dc is being set to 2 as -cp or/and -rc is/are enabled or being enabled | A user tries to set a minimum number of different password characters value that conflicts with password reuse cycle (-rc) and complex password (-cp) settings. |
| CMM security policy disallows -cp disable right now. | A user attempts to disable the complex password (-cp) when the current security level setting does not allow it. |
| CMM security policy disallows -de disable right now. | A user attempts to disable mandatory USERID password change at first login (-de) when the current security level setting does not allow it. |
| CMM security policy disallows -pc disable right now. | A user attempts to disable mandatory password change at first login (-pc) when the current security level setting does not allow it. |
| CMM security policy disallows high level right now. | A user attempts to set the security level to high when the current security level setting does not allow it. |
| CMM security policy disallows legacy level right now. | A user attempts to set the security level to legacy when the current security level setting does not allow it. |
| Getting policy state failed | An error occurs while the CMM is getting the security policy state. |
| Reading account security level failed. | An error occurs while the CMM is reading the account security level. |
| Setting account defaults to high level failed. | An error occurs while the CMM is setting the account security level to -high. |
| Setting account defaults to legacy level failed. | An error occurs while the CMM is setting the account security level to -legacy. |
| The -high option cannot be used with other options. | A user tries to set the account security to high settings while changing individual option values. |
| The -legacy option cannot be used with other options. | A user tries to set the account security to legacy settings while changing individual option values. |
| The account inactivity disable time period must be greater than the account inactivity alert time period. | A user tries to set the account inactivity disable time period to be less than the account inactivity alert time period. |

Table 87. accseccfg command errors (continued)

| Error message | Definition |
|---|---|
| The minimum password change interval must be less than the password expiration period (*number* days or *number* hours).<br>where *number* identifies the minimum password change interval | A user tries to set the -pc option to a value greater than the -pe option. |
| The password expiration period (*number* days or *number* hours) must be greater than the minimum password change interval.<br>where *number* identifies the password expiration period | A user tries to set the -pe option to a value less than the -pc option. |

## advfailover command errors

This topic lists error messages for the advfailover command.

See "Common errors" on page 407 for a list of error messages that apply to all commands. See "advfailover command" on page 49 for information about command syntax and examples of command use.

Table 88. advfailover command errors

| Error message | Definition |
|---|---|
| Operation failed. | An error occurs while the CMM is processing the command. |
| Operation not allowed, since the standby MM is not present. | The user tries to enable advanced failover when there is no standby CMM installed in the Lenovo Flex System chassis. |

## airfilter command errors

This topic lists errors for the airfilter command.

See "Common errors" on page 407 for a list of error messages that apply to all commands. See "airfilter command" on page 51 for information about command syntax and examples of command use.

Table 89. airfilter command errors

| Error message | Definition |
|---|---|
| Error reading air filter settings | An error occurs while the CMM is reading the air filter settings. |

## alarm command errors

This topic lists error messages for the alarm command.

See "Common errors" on page 407 for a list of error messages that apply to all commands. See "alarm command" on page 52 for information about command syntax and examples of command use.

*Table 90. alarm command errors*

| Error message | Definition |
|---|---|
| -clear, -ack, -unack, and -create must be used exclusive of each other | A user tries to issue the alarm command with multiple options that must be used separately. |
| -clear, -ack, -unack, or -create request must be used with this command | A user tries to issue the alarm command without specifying a command option. |
| -i (alarm id) is required when using -*option* option where *option* identifies the command option. | A user tries to issue an alarm command option that requires an alarm ID without specifying an alarm ID. |
| Alarm Description must be enclosed in quotation marks. | A user tries to specify an alarm description without enclosing it in double-quotation marks. |
| Invalid input. -i should have exactly 8 hex digits | A user tries to specify an alarm ID that is not eight hex digits in length. |
| Invalid input -i: There must be all hexadecimal characters | A user tries to specify an alarm ID that contains non-hexadecimal characters. |

## alertcfg command errors

This topic lists errors for the alertcfg command.

There are no unique errors for the alertcfg command. See "Common errors" on page 407 for a list of error messages that apply to all commands. See "alertcfg command" on page 56 for information about command syntax and examples of command use.

## alertentries command errors

This topic lists error messages for the alertentries command.

See "Common errors" on page 407 for a list of error messages that apply to all commands. See "alertentries command" on page 58 for information about command syntax and examples of command use.

*Table 91. alertentries command errors*

| Error message | Definition |
|---|---|
| -test must be used exclusive of other options. | The user tries to issue a command with the -test option at the same time as the other options. |
| An entry cannot be modified and deleted in the same command. | A user tries to modify an entry and delete it in the same command. |
| Enabling the application alert failed. | An error occurs while the CMM is enabling the application alert. |
| Generating test alert failed. | An error occurs while the CMM is generating a test alert. |
| Invalid input. Angle brackets are not allowed in the name field. | A user tries to enter a string parameter containing < or > for the -n (name) command option. |
| Restoring previous configured value for the application alert failed. | An error occurs while the CMM is restoring previous configured value for the application alert. |
| Syntax error. -e can only be used in conjunction with the email argument. | A user tries to enter an invalid email address for the -e command option. |
| The E-mail addresses can not be separated by colon | A user tries to enter email addresses using the wrong syntax. |

*Table 91. alertentries command errors (continued)*

| Error message | Definition |
|---|---|
| The name must be less than 32 characters long. | A user tries to enter too many characters in an input field. |
| When creating a new entry, all options are required. | A required command option is missing when creating a user. |

## autoftp command errors

This topic lists errors for the autoftp command.

See "Common errors" on page 407 for a list of error messages that apply to all commands. See "autoftp command" on page 63 for information about command syntax and examples of command use.

*Table 92. autoftp command errors*

| Error message | Definition |
|---|---|
| Autoftp is disabled, -i, -p, -u and -pw options are invalid. | A user tries to enter -i, -p, -u, or -pw options when the FTP/TFTP/SFTP mode is set to disabled. |
| Error reading data for Terms and Conditions | An error occurs while the CMM is reading the terms and conditions. |
| Invalid input. Address must be less than 64 characters. | A user tries to enter an address that is 64 or more characters long. |
| Invalid input. Password must be less than 64 characters. | A user tries to enter a password that is 64 or more characters long. |
| Invalid input. Userid must be less than 64 characters. | A user tries to enter a user id that is 64 or more characters long. |
| Invalid server address | A user tries to issue the command to a server address that is not valid. |
| Password must be enclosed in quotation marks. Displayed when the argument of option -pw is not quote_ delimited. | A user tries to enter a password without quotation marks. |
| Port number out of range | A user tries to issue the command to a port number that is not in the valid range. |
| Read autoftp configuration failed. | The CMM was unable to read the autoftp configuration. |
| Read autoftp mode failed. | The CMM was unable to read the autoftp mode status. |
| The mode is tftp, -u and -pw options are invalid. | A user tries to enter a user name or password when the mode is set to TFTP. |
| The Terms and Conditions should be accepted first before using this command | A user tries to issue a command before accepting the terms and conditions. |
| User Name must be enclosed in quotation marks. | A user tries to enter a user name without quotation marks. |
| When disabling autoftp, the -i, -p, -u and -pw options are invalid. | A user tries to enter -i, -p, -u, or -pw options when setting the FTP/TFTP/SFTP mode to disabled in the same command. |
| When setting -m to tftp, the -u and -pw options are invalid. | A user tries to enter a user name or password when setting the FTP/TFTP/SFTP mode to TFTP in the same command. |

## baydata command errors

This topic lists error messages for the baydata command.

See "Common errors" on page 407 for a list of error messages that apply to all commands. See "baydata command" on page 66 for information about command syntax and examples of command use.

*Table 93. baydata command errors*

| Error message | Definition |
|---|---|
| Error writing bay data to blade bay *bay*<br>where *bay* is the node bay number. | An error occurs while writing to the identified compute node. |
| Error writing bay data to blade bay *bay*:*slot*<br>where *bay* is the node bay number and *slot* is the subslot. | An error occurs while writing to the identified compute node. |
| Failed to read bay data | An error occurs while reading from a compute node. |
| Invalid bay data | A user attempts to enter bay data that is not valid. |
| Invalid blade bay number | A user attempts to enter a bay number that is 0 or greater than the maximum number of bays in the chassis. |
| Invalid input. The bay data string must be less than 61 characters. | A user attempts to enter a -data option argument for a compute node that exceeds the maximum length of 60 characters. |
| Invalid subslot number | A user attempts to enter a subslot number that is 0 or greater than 2. |
| No blade is present in bay *number*<br>where *number* is the node bay number. | A user attempts to direct a command to a bay that does not contain a compute node. |
| No blade is present in bay *bay*:*slot*<br>where *bay* is the node bay number and *slot* is the subslot. | A user attempts to direct a command to a bay subslot that does not contain a component. |
| The -clear and -data options cannot be used in the same command. | A user attempts to issue a command with both the -clear and -data options specified. |
| The bay data must be quote-delimited. | User enters bay data with -data option for a compute node without double quotation marks. |
| User not authorized to change bay data for bay *bay*<br>where *bay* is the node bay number. | A user attempts to change bay data for a compute node bay that they are not authorized to edit. |

## bootmode command errors

This topic lists errors for the bootmode command.

See "Common errors" on page 407 for a list of error messages that apply to all commands. See "bootmode command" on page 71 for information about command syntax and examples of command use.

*Table 94. bootmode command errors*

| Error message | Definition |
|---|---|
| Boot mode not supported on blade[*x*]<br>where *x* is the number of the node bay. | The command is directed to a compute node that does not support the bootmode feature. |
| Error retrieving the boot mode of this blade. | The CMM is unable read the boot mode of the compute node. |

Table 94. bootmode command errors (continued)

| Error message | Definition |
|---|---|
| Set the blade *bay* boot mode to permanent failed where *bay* is the number of the node bay. | The CMM is unable to set the compute node boot mode to the specified value. |
| Set the blade *bay* boot mode to temporary failed where *bay* is the number of the node bay. | The CMM is unable to set the compute node boot mode to the specified value. |

## bootseq command errors

This topic lists error messages for the bootseq command.

See "Common errors" on page 407 for a list of error messages that apply to all commands. See "bootseq command" on page 73 for information about command syntax and examples of command use.

Table 95. bootseq command errors

| Error message | Definition |
|---|---|
| -i, -g and -s must be configured together | The user tries to set IP address information without specifying all required IP address options. |
| -id must be provided when configuring IP settings | The user tries to set an IP address without specifying a device ID. |
| -seq must be used exclusively with other options | The user attempts to enter multiple command options together that must be used alone. |
| Boot sequence not supported on blade[*x*]<br>where *x* identifies the compute node. | The user tries to enter a boot sequence that is not valid for the compute node target. |
| Boot sequences exceeds max of *max_boot_seqs*<br>where *max_boot_seqs* is the maximum number of boot devices. | The user tries to specify a number of devices in a boot sequence that is more than the maximum allowed. |
| Configuring boot device IP settings of blade[*x*] failed<br>where *x* identifies the compute node. | An error occurs while the CMM is processing the command. |
| Device not found for *id*<br>where *id* is the device ID that identifies the device. | The user tries to specify a device ID that does not exist. |
| Getting boot device list of blade[*x*] failed<br>where *x* identifies the compute node. | An error occurs while the CMM is processing the command. |
| Getting boot sequence of blade[*x*] failed<br>where *x* identifies the compute node. | An error occurs while the CMM is processing the command. |
| No boot device list | The user tries to set the boot sequence without specifying any devices. |
| No duplicate device are allowed | The user tries to set the same device twice in the boot sequence. |
| Setting boot sequence for blade[*x*] failed<br>where *x* identifies the compute node. | An error occurs while the CMM is processing the command. |
| The argument of -id must be numeric | The user tries to enter a parameter value containing non-numeric characters for a command option requiring numeric input. |

## chconfig command errors

This topic lists errors for the chconfig command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “chconfig command” on page 76 for information about command syntax and examples of command use.

*Table 96. chconfig command errors*

| Error message | Definition |
|---|---|
| -li view must be used exclusive of other options | A user tries to view or accept the service advisor terms and conditions when running another command option. |
| All the required information fields must be set before enabling -sa | A user tries to enable the service advisor before configuring all required information. |
| Alternate Contact Email: invalid input. Please make sure your input is not empty and within 128 characters complying with the format in help. | A user tries to enter an incorrectly formatted email address. |
| Alternate Contact Name must be enclosed in quotation marks. | A user tries to enter an alternate contact name that is not enclosed in double quotation marks. |
| Alternate Contact Phone Number Extension: invalid input. Please make sure your input is not empty and 1-30 characters | A user tries to enter an incorrectly formatted phone number extension. |
| Alternate Contact Phonenumber Extension must be enclosed in quotation marks. | A user tries to enter a phone number extension that is not enclosed in double quotation marks. |
| Alternate Contact Phone number: invalid input. Please make sure your input is not empty and 5-30 characters. | A user tries to enter an incorrectly formatted phone number. |
| Alternate Contact Phonenumber must be enclosed in quotation marks | A user tries to enter a phone number that is not enclosed in double quotation marks. |
| Address must be enclosed in quotation marks. | A user tries to enter an address that is not enclosed in double quotation marks |
| City must be enclosed in quotation marks. | A user tries to enter a city name that is not enclosed in double quotation marks |
| IBM Support Center: invalid input. Please input 2 characters ISO country code for the IBM Support Center. | A user tries to enter a country code that is not valid. |
| Contact Company must be enclosed in quotation marks. | A user tries to enter a company name that is not enclosed in double quotation marks. |
| Contact Name must be enclosed in quotation marks. | A user tries to enter a contact name that is not enclosed in double quotation marks. |
| Contact Phone Number Extension: invalid input. Please make sure your input is not empty and 1-30 characters | A user tries to enter an incorrectly formatted phone number extension. |
| Contact Phonenumber Extension must be enclosed in quotation marks | A user tries to enter a phone number extension that is not enclosed in double quotation marks. |
| Email must be enclosed in quotation marks. | A user tries to enter an email that is not enclosed in double quotation marks. |
| Email: invalid input. Please make sure your input is not empty and within 128 characters complying with the format in help. | A user tries to enter an incorrectly formatted email address. |

*Table 96. chconfig command errors (continued)*

| Error message | Definition |
|---|---|
| Error setting -sa | An error occurs while configuring service advisor. |
| Error to enable Service Agent. You have not set all of the required contact Information fields yet. | A user tries to issue a command to enable a service agent that does not have the required contact information set. |
| Fail to get HTTP Proxy settings | A failure occurs while reading the HTTP proxy settings. |
| Fail to read Contact Information | A failure occurs while reading the contact information. |
| Fail to read IBM Support Center | A failure occurs while reading the Lenovo Support Center information. |
| HTTP Proxy is disabled now, you can not change proxy settings, please enable http proxy first. | A user tries to change proxy settings when the HTTP proxy is disabled. |
| Invalid HTTP Proxy location. | A user tries to enter a proxy address that is not a valid IP address or hostname. |
| Invalid input. -loc should be less than 64 characters. | A user tries to enter a proxy address that is 64 or more characters long. |
| Invalid input. -pw should be less than 16 characters. | A user tries to enter a proxy password that is 16 or more characters long. |
| Invalid input. Password should not contain spaces | A user tries to enter a password that contains spaces. |
| Invalid input. User Name must be less than 30 characters. | A user tries to enter a user name that is 30 or more characters long. |
| Invalid input. User Name should not contain spaces. | A user tries to enter a user name that contains spaces. |
| Machine Location Phone number: invalid input. Please make sure your input is not empty and 5-30 characters. | A user tries to enter an incorrectly formatted phone number. |
| Machine Location Phonenumber must be enclosed in quotation marks | A user tries to enter a phone number that is not enclosed in double quotation marks. |
| Postalcode: invalid input. Please make sure your input is 1-9 characters and only contains letters, numbers | A user tries to enter an incorrectly formatted postal code. |
| Read Terms and Conditions failed | An error occurs while reading the terms and conditions. |
| State: invalid input. Please make sure your input is 2-3 characters | A user tired to enter an invalid state code. |
| Terms and conditions is not accepted yet, please view and accept the terms and conditions first. | A user attempts to change the service advisor settings before accepting the terms and conditions. |
| The Terms and Conditions should be accepted first before using this command. | A user attempts to change the service manager settings before accepting the license agreement. |
| Password must be enclosed in quotation marks. | A user tries to enter a password that is not enclosed in double quotation marks. |
| Phone number must be enclosed in quotation marks. | A user tries to enter a phone number that is not enclosed in double quotation marks. |
| Phone number: invalid input. Please make sure your input is not empty and 5-30 characters. | A user tries to enter a phone number that is not valid. |
| Postalcode must be enclosed in quotation marks. | A user tries to enter a postal code that is not enclosed in double quotation marks. |
| User Name must be enclosed in quotation marks. | A user tries to enter a user name that is not enclosed in double quotation marks. |

## chlog command errors

This topic lists errors for the chlog command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “chlog command ” on page 83 for information about command syntax and examples of command use.

*Table 97. chlog command errors*

| Error message | Definition |
|---|---|
| -f must be used exclusive of other options. | The user tries to use the -f option at the same time as other options. |
| -s must be used exclusive of other options. | The user tries to use the -s option at the same time as other options. |
| A call home event with index *number* was not found. where *number* is the decimal number that specifies the serviceable activity log entry that the user is attempting to acknowledge or unacknowledge. | The CMM was unable to find a specified call-home event activity log entry. |
| Error reading data for Terms and Conditions. | An error occurs while the CMM is reading the terms and conditions information. |
| Fail to read Activity Log next entries | The CMM was unable to read the next set of entries in the activity log. |
| Fail to read Service Advisor Activity Log | The CMM was unable to read the call-home event activity log. |
| The Terms and Conditions should be accepted first before using this command | The user attempts to use the command without accepting the terms and conditions. |

## chmanual command errors

This topic lists errors for the chmanual command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “chmanual command” on page 86 for information about command syntax and examples of command use.

*Table 98. chmanual command errors*

| Error message | Definition |
|---|---|
| -test must be used exclusive of other options | The user attempts to run this command with other options in addition to -test. |
| Error generating a manual Call Home | This command fails when the user attempts the manual call home operation. |
| Error generating a test Call Home | This command fails when the user attempts the test call home operation. |
| Error reading data for Terms and Conditions | An error occurs while reading terms and conditions data. |
| Problem description must be enclosed in quotation marks | The user attempts to run this command when the problem description is not enclosed in quotation marks. |
| Test Call Home should be operated on SYSTEM target | The user attempts to use this command when the command is not targeted on system' for test call home. |

*Table 98. chmanual command errors (continued)*

| Error message | Definition |
|---|---|
| The Service Advisor is disabled now, please enable it before calling 'chmanual' | The user attempts to use this command before the service advisor is enabled. |
| The Terms and Conditions should be accepted first before using this command | The user attempts to use the command without accepting the terms and conditions. |

## cimsub command errors

This topic lists error messages for the cimsub command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “cimsub command ” on page 88 for information about command syntax and examples of command use.

*Table 99. cimsub command errors*

| Error message | Definition |
|---|---|
| Error reading CIM subscription info | An error occurs during data collection. |

## cin command errors

This topic lists error messages for the cin command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “cin command ” on page 91 for information about command syntax and examples of command use.

*Table 100. cin command errors*

| Error message | Definition |
|---|---|
| -id cannot be the same as the blade management VLAN ID. Please try again. | A user tries to enter a command with a VLAN ID which is the same as the VLAN ID of the compute node management. |
| -ip cannot be multicast. Please try again. | A user issues a command with an IP address which is the same as the IP address of the multicast. |
| -ip cannot be the same as the CMM IP address. Please try again | A user tries to enter a command with an IP address which is the same as the IP address of the CMM. |
| An error occurred while changing CIN global status setting | An error occurs while user is changing CIN global status setting. |
| An error occurred while clearing CIN entry | An error occurs while the user is clearing a CIN entry. |
| An error occurred while enabling/disabling CIN entry. | An error occurs while the user is enabling/disabling a CIN entry. |
| An error occurred while setting CIN entry. | An error occurs while configuring a CIN entry. |
| Both -id and -ip are required for adding a CIN entry. | A user tries to enter a command to add an entry without both -id and -ip options. |
| CIN blade pair TLV get failed | An error occurs while the CMM is getting CIN compute node configuration parameters. |
| CIN global TLV get failed. | An error occurs while the CMM is getting a CIN global configuration parameter. |

*Table 100. cin command errors (continued)*

| Error message | Definition |
|---|---|
| CIN command failed. | An error occurs while the CMM is executing a CIN command. |
| cin -*index* -en *state* cannot be used with other options. where<br>• *index* identifies the cin index entry<br>• *state* is on or off | The user tries to enter a command with the -en option with along with other options. |
| Duplicate CIN (-id, 0.0.0.0) pairs are not allowed. Please try again. | A user tries to enter a command with a duplicated -id/ 0.0.0.0 pair. |
| Duplicate -ip is not allowed. Please try again. | A user tries to enter a command with a duplicated IP address. |
| Getting CMM failed | System is unable to locate a CMM. |
| Internal error checking CIN entry. | An error occurs while the system checks user input for the CIN entry configuration. |
| Internal error getting CIN entry | An error occurs while the CMM is getting CIN entry configuration parameters. |
| Invalid index parameter. Input must be numeric. | A user tries to enter a command with a non-numeric index. |
| Invalid index parameter. Input out of range. | A user tries to enter a command with an index which is out of range. |
| Invalid IP argument for an option. Enter 4 bytes separated by 3 dots. | A user tries to enter a command argument for IP address option which is invalid because it is too long, too short, or not numeric. |
| Invalid IP argument for an option. Too many bytes. | A user tries to enter a command with an invalid argument for IP address option which has more than four parts. |
| Invalid IP argument for an option. Too few bytes | A user tries to enter a command with an invalid argument for IP address option which has fewer than four parts. |
| Invalid IP argument for an option. Each byte has to be in the range (0-255). | A user tries to enter a command with an invalid argument for IP address option, each part of which is not in the range of 0-255. |
| Invalid option argument for -global -en: | A user issues a command with an invalid argument for -global -en option. |
| No CMM found | System is unable to locate a CMM. |
| No primary CMM found | System is unable to locate the primary CMM. |

## cinstatus command errors

This topic lists error messages for the cinstatus command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “cinstatus command ” on page 97 for information about command syntax and examples of command use.

Table 101. cinstatus command errors

| Error message | Definition |
|---|---|
| Getting CMM failed | System is unable to locate a CMM. |
| No CMM found | System is unable to locate a CMM. |
| No primary CMM found | System is unable to locate the primary CMM. |

## clear command errors

This topic lists error messages for the clear command.

See "Common errors" on page 407 for a list of error messages that apply to all commands. See "clear command" on page 98 for information about command syntax and examples of command use.

Table 102. clear command errors

| Error message | Definition |
|---|---|
| Disabling failover failed | An error occurs while disabling failover. |
| Firmware update is in progress. Try again later. | The user tries to reset the CMM to its default configuration during a firmware update. The error message displays and the CMM configuration does not reset. |
| Internal error resetting to defaults. | An error occurs while the CMM is resetting the CMM to its default configuration. The error message displays and the CMM configuration does not reset. |
| Not supported by this type of I/O module. Type env -h for help on changing targets | A user tries to run a command option on an I/O module that does not support it. |
| This command cannot be issued right now. If you still want to clear the primary CMM, please use 'clear -cnfg -o' to override this warning. | A condition exists that is preventing the CMM from being cleared. You can either wait and try the command again or force the CMM to clear immediately using the `clear -cnfg -o` override option. |
| This command cannot be issued right now. The standby CMM is in an unknown state, and a reset might result in a failover. If you still want to clear the primary CMM, please use 'clear -cnfg -o' to override this warning. | A condition exists that is preventing the CMM from being cleared. You can either wait and try the command again or force the CMM to clear immediately using the `clear -cnfg -o` override option. |
| This command cannot be issued right now. The primary CMM is verifying the code level on the standby CMM. Please try again later. | A user tries to issue a command to the CMM when it is unavailable. |
| This command cannot be issued right now. The standby CMM is flashing, and resetting the primary CMM to defaults might result in a failover. Please try again later. | A user tries to reset the primary CMM to defaults while the standby CMM is unable to support failover. |
| This command cannot be issued right now. The standby CMM is in a post-flash initialization state, and resetting the primary CMM to defaults might result in a failover. If you still want to reset the primary CMM, please use 'clear -cnfg -o' to override this warning. | A user tries to reset the primary CMM to defaults while the standby CMM is unable to support failover. |
| This command cannot be issued right now. The primary CMM is initializing, and a reset might result in a failover. If you still want to clear the primary CMM, please use 'clear -cnfg -o' to override this warning. | A condition exists that is preventing the CMM from being cleared. You can either wait and try the command again or force the CMM to clear immediately using the `clear -cnfg -o` override option. |

## clearlog command errors

This topic lists error messages for the clearlog command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “clearlog command” on page 100 for information about command syntax and examples of command use.

*Table 103. clearlog command errors*

| Error message | Definition |
|---|---|
| Error clearing the event log. | An error occurs while the CMM is clearing the event log. |

## config command errors

This topic lists error messages for the config command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “config command” on page 102 for information about command syntax and examples of command use.

*Table 104. config command errors*

| Error message | Definition |
|---|---|
| Contact must be enclosed in quotation marks. | The user tries to enter a CMM Contact without enclosing it in double quotes. |
| Invalid input. Contact may not contain angle brackets. | The user tries to enter a CMM contact containing angle brackets ("<" and ">"). |
| Invalid input. Location may not contain angle brackets. | The user tries to enter a CMM location containing angle brackets ("<" and ">"). |
| Invalid input. Lowest U must be 2 digit number | The user tries to enter a U number that is not two digits in length. |
| Invalid input. Lowest U must be numeric | The user tries to enter a U number that is non-numeric. |
| Invalid input. Name contains invalid characters | The user tries to enter a name containing characters that are not valid. |
| Invalid input. Name must be less than 16 characters. | The user tries to enter a name that is more than 15 characters in length. |
| Invalid input. Name may not contain angle brackets. | The user tries to enter a compute node name that contains angle brackets: "<" or ">". |
| Invalid input. Name can only contain alphanumeric characters, underscores, hyphens, pound signs, and periods. | The user tries to enter a name for the CMM that is not valid. |
| Invalid input. Rack contains invalid characters | The user tries to enter a rack identifier containing characters that are not valid. |
| Invalid input. Room contains invalid characters | The user tries to enter a room identifier containing characters that are not valid. |
| Location must be enclosed in quotation marks. | The user tries to enter a CMM Location without enclosing it in double quotes. |
| Rack must be enclosed in quotation marks | The user tries to enter a rack identifier without beginning and ending double quotes. |

Table 104. config command errors (continued)

| Error message | Definition |
|---|---|
| Reading SNMPv1/SNMPv3 status failed. | An internal errors occurs while the CMM is reading the SNMPv1/v3status. |
| Room must be enclosed in quotation marks | The user tries to enter a room identifier without beginning and ending double quotes. |
| System location and contact must be defined when SNMPv1 or SNMPv3 agent is enabled. | The user tries to undefine the system location or contact information while an SNMPv1 or SNMPv3 agent is enabled. |

## console command errors

This topic lists error messages for the console command.

See "Common errors" on page 407 for a list of error messages that apply to all commands. See "console command" on page 107 for information about command syntax and examples of command use.

Table 105. console command errors

| Error message | Definition |
|---|---|
| Error entering console mode. | An error occurs while the CMM is trying to establish an SOL connection. |
| Global SOL is not enabled | SOL is not enabled globally. |
| SOL is not ready | The compute node is not available, or when a socket needed to establish a connection to the compute node is not available. |
| SOL on blade is not enabled | SOL is not enabled on the compute node where the user is trying to start an SOL session. |
| SOL not supported on blade[*node_number*]<br>where *node_number* identifies the compute node. | The user tries to initiate an SOL session with a compute node that does not support this feature. |
| SOL session is already active | The user cannot start an SOL session with a compute node because an SOL session with that compute node is already in progress. |
| The current VLAN configuration prohibits user access to SOL | The user tries to initiate an SOL session via a VLAN that does not allow SOL access. |
| The maximum number of sessions to this blade has been reached. | The compute node has no available sessions for a user to connect to. |
| There is no blade present in that bay | The user tries to direct a command option to a compute node bay that does not contain a compute node. |

## coolingzones command errors

This topic lists error messages for the coolingzones command.

See "Common errors" on page 407 for a list of error messages that apply to all commands. See "coolingzones command" on page 108 for information about command syntax and examples of command use.

*Table 106. coolingzones command errors*

| Error message | Definition |
|---|---|
| Getting max slots of target failed | An error occurs while getting the maximum number of slots in the command target. |
| Invalid zone option. It must be two alphanumeric characters | The user attempts to issue the command for a cooling zone that is invalid. |
| Invalid zone option. The first character must be 'z' | The user attempts to issue the command without specifying the letter “z” as the first character of the cooling zone. |
| The second character must be a digit in range of 1 to *max* where *max* defines the highest cooling zone number that is allowed. | The user attempts to issue the command without specifying the a number between 1 and the maximum allowed value, inclusive, as the second character of the cooling zone. |
| Getting cooling zone information failed | An error occurs while getting cooling zone information. |
| Getting cooling zones status failed | An error occurs while getting cooling zone status. |
| No cooling zone information available | An error occurs while getting cooling zone information. |

## crypto command errors

This topic lists errors for the crypto command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “crypto command” on page 110 for information about command syntax and examples of command use.

*Table 107. crypto command errors*

| Error message | Definition |
|---|---|
| -cs cannot be changed from tls1.2 to tls1.2srv when -m is set to nist800-131a | A user attempts to change the cipher suite to `tls1.2srv` that is not compatible with the current cipher mode of `nist800-131a`.<br>When the CMM is configured for NIST Strict operation (mode is `nist800-131a`and cipher suite is `tls1.2`), users can not change to NIST Custom operation (mode is `nist800-131a` and cipher suite is `tls1.2svr`). |
| -cs cannot be set to legacy while -m is set to nist800-131a | A user attempts to set -cs to legacy while either -m is set to nist800-131a, or -m is being set to nist800-131a. |
| -m cannot be set to nist800-131a while -cs is set to legacy | A user attempts to set -m to nist800-131a while -cs is set to legacy. |
| A cryptographic mode change is disallowed at this time. Firmware update is in progress. Try again later. | A user attempts to make a cryptographic mode change while the CMM is unable to modify settings. |
| A cryptographic mode change is disallowed at this time. The standby CMM is in an unknown state, and a reset might result in a failover. | A user attempts to make a cryptographic mode change while the CMM is unable to modify settings. |
| A cryptographic mode change is disallowed at this time. The primary CMM is verifying the code level on the standby CMM. | A user attempts to make a cryptographic mode change while the CMM is unable to modify settings. |
| A cryptographic mode change is disallowed at this time. The standby CMM is flashing. | A user attempts to make a cryptographic mode change while the CMM is unable to modify settings. |

Table 107. crypto command errors (continued)

| Error message | Definition |
|---|---|
| A cryptographic mode change is disallowed at this time. The primary CMM is initializing. | A user attempts to make a cryptographic mode change while the CMM is unable to modify settings. |
| A cryptographic mode change is disallowed at this time. The standby CMM is in a post-flash initialization state. | A user attempts to make a cryptographic mode change while the CMM is unable to modify settings. |
| Configurations options blocking transition to NIST Strict | Other settings prevent the CMM from transitioning to nist800-131a cryptographic mode. |
| Crypto mode change not permitted. The following nodes require an update to the latest blade firmware: *node*<br>where *node* identifies the compute nodes requiring a firmware update. | A user attempts to change cryptographic settings when compute node firmware requires an update to support the change. |
| Disabling failover failed. | Disabling CMM failover fails while the CMM attempts to restart. |
| External LDAP certificate for profiles has invalid params | Other settings prevent the CMM from transitioning to nist800-131a cryptographic mode. |
| External LDAP certificate in slot *number* has invalid params<br>where *number* identifies the slot with invalid parameters. | Other settings prevent the CMM from transitioning to nist800-131a cryptographic mode. |
| FSM User *number* has non-compliant SNMP properties<br>where *number* identifies the user with properties that are not compliant. | Other settings prevent the CMM from transitioning to nist800-131a cryptographic mode. |
| Restarting CMM failed. | The CMM failed to restart. |
| Restarting the CMM now for changes to -m to take effect. | Advisory message indicating that the CMM is restarting. |
| SSH key *key* for user *user* has invalid length<br>where *key* identifies the invalid length key and *user* identifies the user assigned this key. | Other settings prevent the CMM from transitioning to nist800-131a cryptographic mode. |
| SSL clients cipher suites legacy compatibility | Other settings prevent the CMM from transitioning to nist800-131a cryptographic mode. |
| TLS minimum version change not permitted. The following nodes require an update to the latest blade firmware: *node*<br>where *node* identifies the compute nodes requiring a firmware update. | A user attempts to change cryptographic settings when compute node firmware requires an update to support the change. |
| User *number* has non-compliant SNMP properties<br>where *number* identifies the user with properties that are not compliant. | Other settings prevent the CMM from transitioning to nist800-131a cryptographic mode. |

## date command errors

This topic lists error messages for the date command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “date command” on page 113 for information about command syntax and examples of command use.

Table 108. date command errors

| Error message | Definition |
|---|---|
| '-v' must be used with 'date -tz all' only | A user tries to issue a command with the -v option with an option other than -tz. |
| 'date -tz all' must be used exclusive of other options except '-v' | A user tries to issue a command with the -tz option at the same time as other options (other than -v). |
| Getting current date and time failed | An error occurred while the system was retrieving current date and time information. |
| Getting time zones failed | An error occurred while the system was retrieving time zone information. |
| Invalid value for day | A user tries to enter an invalid argument for day in the date (-d) option. |
| Invalid value for hours | A user tries to enter an invalid argument for hours in the time (-t) option. |
| Invalid value for minutes | A user tries to enter an invalid argument for minutes in the time (-t) option. |
| Invalid value for month | A user tries to enter an invalid argument for month in the date (-d) option. |
| Invalid value for seconds | A user tries to enter an invalid argument for seconds in the time (-t) option. |
| Invalid value for year | A user tries to enter an invalid argument for year in the date (-d) option. |
| No time zone found | An error occurred while the system was retrieving time zone information. |
| NTP is enabled. Please use 'ntp' command to disable NTP before configuring date or time | A user tries to configure date or time setting while the system is configured to use Network Time Protocol (NTP). |
| The year has to be between *min* and *max*<br>where *min* and *max* define the range of years that is allowed. | A user tries to enter a year that is outside of the allowed range. |

## dhcpinfo command errors

This topic lists errors for the dhcpinfo command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “dhcpinfo command” on page 115 for information about command syntax and examples of command use.

Table 109. dhcpinfo command errors

| Error message | Definition |
|---|---|
| Advanced failover must be enabled before viewing the standby MM's DHCPv6 config. | A user tries to view the configuration of the standby CMM when advanced failover is disabled. |
| DHCP is disabled | The DHCP assigned configuration can not be retrieved because DHCP is disabled. |
| DHCPv6 information is not available. | DHCPv6 is enabled, but the command target is not receiving any DHCPv6 settings. |
| DHCPv6 is disabled | The DHCPv6 assigned configuration can not be retrieved because DHCPv6 is disabled. |

Table 109. dhcpinfo command errors (continued)

| Error message | Definition |
|---|---|
| Error reading network configuration | An error occurs while the CMM is reading the network configuration. |
| IPv6 is disabled | The DHCPv6 assigned config can not be retrieved because IPv6 is disabled. |
| This management network interface is not installed. | A user issues the dhcpinfo command to a compute node that does not support a management network interface. |
| Unknown interface | A user tries to direct a command to an invalid network interface. |

## displaylog command errors

This topic lists error messages for the displaylog command.

See "Common errors" on page 407 for a list of error messages that apply to all commands. See "displaylog command" on page 119 for information about command syntax and examples of command use.

Table 110. displaylog command errors

| Error message | Definition |
|---|---|
| (There are no more entries in the event log.) | There are no more event log entries to display. |
| -f and -a cannot be used at the same time. | The user tries to use the -f and -a options in the same command. |
| -filters must be used exclusive of the other options | The user tries to set the -filters option at the same time as other options. |
| -lse option must be used exclusive of the other options | The user tries to set the -lse option at the same time as other options. |
| -u option must be used exclusive of the other options. | The user tries to set the -u option at the same time as other options. |
| Cannot open file: *filename*<br>where *filename* is the name of the file that was entered when the error occurred. | An error occurs while the CMM is trying to open a file. |
| Couldn't resolve or connect to the host | An error occurs while trying to establish a connection with the host. |
| Downloading to *URL* failed<br>where *URL* is the location that was entered when the error occurred. | An error occurs when downloading to the specified URL. |
| Duplicate date filter: *filter*<br>where *filter* is the duplicate date filter that was entered. | The user tries to use duplicate date filters. |
| Duplicate call home filter: *filter*<br>where *filter* is N, C, or S. | The user tries to use duplicate call-home filters. |
| Duplicate severity filter: *filter*<br>where *filter* is the duplicate severity filter that was entered. | The user tries to use duplicate severity filters. |
| Duplicate source filter: *filter*<br>where *filter* is the duplicate source filter that was entered. | The user tries to use duplicate source filters. |
| Error parsing event log. | An error occurs while the CMM is parsing the event log. |

Table 110. displaylog command errors (continued)

| Error message | Definition |
|---|---|
| Error reading event log. | An error occurs while the CMM is reading the event log. |
| File already exists | A user tries to create a file that already exists. |
| File transfer already in progress | A user tries to initiate a file transfer while one is already in process. |
| File transfer failed abnormally. | An error occurs during a file transfer. |
| File transfer failed. *error_info*<br>where *error_info* provides specific information about the error. | An error occurs during a file transfer. |
| Incomplete or malformed URL. | The user tries to use an invalid URL. |
| Invalid date filter: *filter*<br>where *filter* is the invalid date filter that was entered. | The user tries to use an invalid date filter. |
| Invalid call home filter: *filter*<br>where *filter* is the invalid filter that was entered. | The user tries to use an invalid call-home filter. |
| Invalid severity filter: *filter*<br>where *filter* is the invalid severity filter that was entered. | The user tries to use an invalid severity filter. |
| Invalid source filter: *filter*<br>where *filter* is the invalid source filter that was entered. | The user tries to use an invalid source filter. |
| Invalid username or password | The user tries to enter an invalid user name or password. |
| Log not found. | An error occurs when the CMM attempts to locate the log. |
| Please provide a file name at the end of the URL | The user tries to enter a URL without the required file name. |
| Protocol string length exceeds max of 8 | The user tries to enter a protocol string that is too long. |
| Reading log entries failed. | An error occurs while the CMM is reading log entries. |
| The connection was terminated or timed out | A user tries to initiate a command after the connection has timed out. |
| The file does not exist on the server | A user tries to access a file that does not exist. |
| There is not enough space to save the file | A user tries to save a file larger than the free space that is available. |
| The Server responded in an unexpected way | An error occurs during command processing. |
| The Server sent a file that was not the same size as it's header described | An error occurs during file transfer. |
| There was a problem downloading the file | The user does not have the authority for downloading or an error occurs when downloading. |
| Transfer failed due to transfer library error | An error occurs during file transfer. |
| Unknown error occurred | An error occurs while processing the command. |
| Unsupported protocol | The user tries to issue a command using a protocol that is not supported. |
| URL is not properly formatted | The user tries to enter a URL that is not of the correct format. |

Table 110. displaylog command errors (continued)

| Error message | Definition |
|---|---|
| URL syntax checking failed | The user tries to enter a command that has a syntax error. |
| User does not have permission to access the requested file | The user tries to access a file without being assigned the necessary permissions. |

## displaysd command errors

This topic lists error messages for the displaysd command.

See "Common errors" on page 407 for a list of error messages that apply to all commands. See "displaysd command" on page 125 for information about command syntax and examples of command use.

Table 111. displaysd command errors

| Error message | Definition |
|---|---|
| -mmstat can not be used with other options | A user tries to use the -mmstat command option at the same time as other command options. |
| -o must be used with -u | A user tries to override warnings without saving service data. |
| Couldn't resolve or connect to the host | An error occurs while trying to establish a connection with the host. |
| Downloading to *URL* failed.<br>where *URL* is the URL specified as a download location. | An error occurs when the user tries to download to a specified URL. |
| Error retrieving blade type. | The CMM fails to read the compute node type. |
| Error transferring file. | An unspecified error occurs. |
| File already exists | A user tries to create a file that already exists. |
| File transfer already in progress | A user tries to initiate a file transfer while one is already in process. |
| Generating service data file failed | An error occurs while generating service data. |
| Incomplete or malformed URL. | The user tries to use an invalid URL. |
| Invalid username or password | The user tries to enter an invalid user name or password. |
| Please provide a file name at the end of the URL | The user tries to enter a URL without the required file name. |
| Protocol string length exceeds max of 8 | The user tries to enter a protocol string that is too long. |
| Read/write command error. | An error occurs while the CMM is processing the command. |
| Service data generation failed | An error occurs while generating service data. |
| Service data generation was successful but an error was encountered packaging the results | An error occurs while generating service data. |
| The connection was terminated or timed out | A user tries to initiate a command after the connection has timed out. |
| The file does not exist on the server | A user tries to access a file that does not exist. |
| The format of the received data is wrong. | The CMM receives wrongly formatted data. |

*Table 111. displaysd command errors (continued)*

| Error message | Definition |
|---|---|
| The Server responded in an unexpected way | An error occurs during command processing. |
| The Server sent a file that was not the same size as it's header described | An error occurs during file transfer. |
| The standby CMM is not fully initialized at this moment and is unable to transfer its service data to the primary CMM. Please try again later, or use the -o flag to override this warning. | A user tries to issue a command to the standby CMM when it is unavailable. |
| There is not enough space to save the file | A user tries to save a file larger than the free space that is available. |
| There was a problem downloading the file | The user does not have the authority for downloading or an error occurs when downloading. |
| Transfer failed due to transfer library error | An error occurs during file transfer. |
| Unknown error occurred | An error occurs while processing the command. |
| Unsupported protocol | The user tries to issue a command using a protocol that is not supported. |
| URL is not properly formatted | The user tries to enter a URL that is not of the correct format. |
| URL syntax checking failed | The user tries to enter a command that has a syntax error. |
| User does not have permission to access the requested file | The user tries to access a file without being assigned the necessary permissions. |

## dns command errors

This topic lists error messages for the dns command.

See "Common errors" on page 407 for a list of error messages that apply to all commands. See "dns command" on page 127 for information about command syntax and examples of command use.

*Table 112. dns command errors*

| Error message | Definition |
|---|---|
| -on and -off cannot both be used in the same command. | A user tries to enable and disable DNS in the same command. |
| At least one address is required to enable DNS. | A user tries to enable DNS without configuring at least one address. |
| Configuring DNS failed | An error occurs while configuring DNS. |
| Disabling DNS failed | An error occurs while disabling DNS. |
| Enabling DNS failed | An error occurs while enabling DNS. |
| Getting DNS configuration failed | An error occurs while retrieving DNS information. |
| IPv6 configuration changes will not take effect until IPv6 is enabled. | A user attempts to configure the IPv6 DNS settings while IPv6 is disabled. |
| Reading status of DNS failed. | An error occurs while the CMM is reading the DNS state. |

## env command errors

This topic lists errors for the env command.

There are no unique errors for the env command. See "Common errors" on page 407 for a list of error messages that apply to all commands. See "env command" on page 131 for information about command syntax and examples of command use.

## ethoverusb command errors

This topic lists errors for the ethoverusb command.

See "Common errors" on page 407 for a list of error messages that apply to all commands. See "ethoverusb command" on page 136 for information about command syntax and examples of command use.

*Table 113. ethoverusb command errors*

| **Error message** | **Definition** |
|---|---|
| Blade SP's command interface on Ethernet-over-USB is not supported on blade *node_number*<br>where *node_number* identifies the compute node. | The command is directed to a compute node that does not support Ethernet-over-USB. |
| Notice: This operation may take a short while to complete. Please view the status to determine when the operation has completed. | Confirmation message indicating that the command is processing and might take a short time to complete. |

## events command errors

This topic lists errors for the events command.

See "Common errors" on page 407 for a list of error messages that apply to all commands. See "events command" on page 138 for information about command syntax and examples of command use.

*Table 114. events command errors*

| **Error message** | **Definition** |
|---|---|
| -add and -rm should be used exclusively of each other. | A user attempts to issue a command with both options -add and -rm. |
| Call Home Exclusion List has reached its maximum size of *max* entries. No more events can be added to the list.<br>where *max* is a decimal number. | A user attempts to add an entry while Call Home Exclusion List has reached its maximum size. |
| Error reading ftp/tftp of Service Data configuration. | An error occurs while the CMM is reading the FTP/TFTP service data configuration. |
| Error reading data for Terms and Conditions. | An error occurs while the CMM is reading the terms and conditions data. |
| Event *id* already exists in Call Home Exclusion List.<br>where *id* is a hexadecimal number that identifies a call-home event. | A user attempts to add an entry which already exists in Call Home Exclusion List. |
| Event *id* does not exist in the Call Home Exclusion List.<br>where *id* is a hexadecimal number that identifies a call-home event. | A user attempts to remove an entry which does not exist in Call Home Exclusion List. |

Table 114. events command errors (continued)

| Error message | Definition |
|---|---|
| Event *id* is invalid to be added into Call Home Exclusion List.<br>where *id* is a hexadecimal number that identifies a call-home event. | A user attempts to add an entry with an invalid event id. |
| ftp/tftp of Service Data must be enabled before using this command. | A user attempts to issue an `events` command while the FTP/TFTP Report of Service Data is disabled |
| Read Call Home Exclusion List failed. | An error occurs while the CMM is reading the Call Home Exclusion List. |
| The terms and conditions should be accepted first before using this command. | A user attempts to issue an `events` command before the terms and conditions have been accepted. |

## exit command errors

This topic lists errors for the exit command.

There are no unique errors for the exit command. See “Common errors” on page 407 for a list of error messages that apply to all commands. See “exit command” on page 141 for information about command syntax and examples of command use.

## files command errors

This topic lists error messages for the files command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “files command” on page 141 for information about command syntax and examples of command use.

Table 115. files command errors

| Error message | Definition |
|---|---|
| Directory does not exist. | The user tries to enter a directory that does not exist. |
| Error deleting file *filename*<br>where *filename* is the name of the file that was entered for deletion. | An error occurs while the CMM is trying to delete a file. |
| Error reading file list. | An error occurs while the CMM is reading the directory file list. |
| Error reading file system space. | An error occurs while the CMM is reading the file system space. |
| Error reading first file in dir *directory*.<br>where *directory* is the name of the directory that was entered. | An error occurs while the CMM is reading the first file in the directory. |
| File index out of sequence. | An error occurs while the CMM is reading the index. |
| File list exhausted. | An error occurs while the CMM is reading the file list. |
| File not found. | The specified file is not found. |
| Filename must be less than 256 characters | The user tries to enter a filename that is longer than 256 characters. |
| General, unknown error. | A command is rejected for unknown reasons. |

Table 115. files command errors (continued)

| Error message | Definition |
|---|---|
| Invalid command sent. | The user tries to enter an invalid command. |
| Invalid directory, filename. | The user tries to enter an invalid directory and filename. |
| Invalid file or directory name. | The user tries to enter an invalid directory or filename. |
| The directory name must be less than 256 characters. | A user tries to enter a directory name that is more than 256 characters in length. |
| Unknown caller id. | The caller ID is not recognized. |
| Unknown command. | The user tries to enter a command that is not recognized. |
| Unknown directory path. | The user tries to enter a directory path that is not recognized. |

## fod command errors

This topic lists errors for the fod command.

See "Common errors" on page 407 for a list of error messages that apply to all commands. See "fod command" on page 143 for information about command syntax and examples of command use.

Table 116. fod command errors

| Error message | Definition |
|---|---|
| Error getting license key information | An error occurs while reading features on demand license key information. |
| Error getting licenses | An error occurs while reading features on demand license information. |
| Error reading data | An error occurs while reading features on demand information. |
| Getting switch[*x*] licenses failed<br>where *x* is the I/O-bay that identifies the I/O module. | An error occurs while reading the license information for an I/O module. |
| Not supported by this type of I/O module. Type env -h for help on changing targets | A user tries to initiate features on demand for an I/O module that does not support it. |

## fruactlog command errors

This topic lists errors for the fruactlog command.

See "Common errors" on page 407 for a list of error messages that apply to all commands. See "fruactlog command" on page 144 for information about command syntax and examples of command use.

Table 117. fruactlog command errors

| Error message | Definition |
|---|---|
| Getting FRU activity log failed | An error occurs while trying to access the FRU activity log. |
| No FRU activity log found | No module activity log is found in the FRU activity log. |

## fsmcm command errors

This topic lists errors for the fsmcm command.

There are no unique errors for the fsmcm command. See “Common errors” on page 407 for a list of error messages that apply to all commands. See “fsmcm command” on page 145 for information about command syntax and examples of command use.

## fuelg command errors

This topic lists error messages for the fuelg command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “fuelg command” on page 147 for information about command syntax and examples of command use.

*Table 118. fuelg command errors*

| Error message | Definition |
|---|---|
| -pme can not be 'none' when configuring -spl | The user attempts set the chassis power management and capping to none when a static power limit value is specified. |
| -pme must be other than 'none' when configuring -spl | The user attempts set the chassis power management and capping to none when a static power limit value is specified. |
| -pme must be provided when configuring -spl | The user attempts to specify a static power limit value without setting the chassis power management and capping value to static. |
| -ps and -dps cannot be enabled at the same time. | The user attempts to enable -ps and -dps at the same time. |
| -spl must be numeric if a percentage, or numeric with a 'W' appended if a wattage | The user attempts to enter a value that is in the wrong format for the -spl command option. |
| -spl must be provided when configuring -pme other than 'none' | The user attempts set the chassis power management and capping to static without specifying a static power limit value. |
| A power module failure in domain *domain_number* can result in an immediate shutdown.<br>where *domain_number* identifies the power domain. | A power supply fails and the domain in which it is installed loses redundancy. The Lenovo Flex System chassis might turn itself off, based on the power management configuration. |
| Blade must be powered on to enable/disable dps. | The user attempts to enable or disable dynamic power server mode for a compute node while its power is off. |
| Blade must be powered on to enable/disable fpop | The user attempts to enable or disable favoring performance over power for a compute node while its power is off. |
| Blade must be powered on to enable/disable pme | The user attempts to enable or disable power management and capping for a compute node while its power is off. |
| Blade must be powered on to enable/disable ps | The user attempts to enable or disable static low power saver mode for a compute node while its power is off. |
| Blade must be powered on to set pcap | The user attempts to set the power capping value for a compute node while its power is off. |

*Table 118. fuelg command errors (continued)*

| Error message | Definition |
|---|---|
| Checking if power is preallocated to switch[*number*] failed.<br>where *number* identifies the I/O-bay number. | An error occurs while the CMM is checking if power is preallocated for the specified I/O module. |
| Effective CPU Speed not available. | An error occurs while the CMM is reading the effective CPU Speed. |
| Error reading blade power management capability. | An error occurs while the CMM is reading the compute node power management capability. |
| Error reading hot air recirculation data | An error occurs while the CMM is reading the hot air recirculation data. |
| Error reading runtime blade capability | An error occurs while the CMM is reading the runtime capability for a compute node. |
| Error reading soft minimum. | An error occurs while the CMM is reading the soft minimum value. |
| Error reading soft minimum, using guaranteed minimum instead. | An error occurs while the CMM is reading the soft minimum value. |
| Error writing data for the option -pme<br>Please make sure the blade is powered on | The user attempts to enable power management and capping for a compute node that is turned off. |
| Getting blade health state parameters failed. | An error occurs while the CMM is reading the compute node health state parameters. |
| Getting blade pcap maximum value failed. | An error occurs while the CMM is reading the compute node power cap maximum value. |
| Getting blade pcap minimum value failed. | An error occurs while the CMM is reading the compute node power cap minimum value. |
| Getting blade power cap level failed. | An error occurs while the CMM is reading the compute nodepower cap level. |
| Getting Chassis Power Cap Range failed | An error occurs while the CMM is reading the chassis power cap level. |
| Getting domain latest power sample failed. | An error occurs while the CMM is reading the latest power domain sample. |
| Getting duty cycle numbers failed. | An error occurs while the CMM is reading the duty cycle numbers. |
| Getting duty cycle numbers of blade[*node_number*] failed.<br>where *node_number* identifies the compute node. | An error occurs while the CMM is reading the duty cycle numbers of specified compute node. |
| Getting dynamic power management capability of blade [*node_number*] failed.<br>where *node_number* identifies the compute node. | An error occurs while the CMM is reading the dynamic power management capability of specified compute node. |
| Getting information of power[*number*] failed.<br>where the *number* identifies the specified power supply. | An error occurs while the CMM is reading data of specified power supply. |
| Getting name of mm[*number*] failed<br>where the *number* identifies the specified CMM bay number. | An error occurs while the CMM is reading the CMM name. |
| Getting power allocation for blade[*node_number*] failed<br>where *node_number* identifies the compute node. | An error occurs while the CMM is reading the power allocation information of the specified compute node. |

*Table 118. fuelg command errors (continued)*

| Error message | Definition |
|---|---|
| Getting power cap level for blade[*node_number*] failed<br>where *node_number* identifies the compute node. | An error occurs while the CMM is reading the power cap level of the specified compute node. |
| Getting power management policy for domain *domain_number* failed<br>where *domain_number* is the number of the domain that was entered. | An error occurs while the CMM is reading the power management policy of the specified domain. |
| Getting power state of blade[*node_number*] failed.<br>where *node_number* identifies the compute node. | An error occurs while the CMM is reading the power state of specified compute node. |
| Getting power values for blower[*number*] failed.<br>where the *number* identifies the location of the component. | An error occurs while the CMM is reading the power values of specified chassis cooling unit. |
| Getting power values of Fanmux slot failed | An error occurs while the CMM is reading the power values of a fan logic module. |
| Getting power values for MM[*number*] failed.<br>where the *number* identifies the location of the component. | An error occurs while the CMM is reading the power values of specified CMM. |
| Getting power values for switch[*number*] failed.<br>where the *number* represents the specified I/O module. | An error occurs while the CMM is reading the power values of specified I/O module. |
| Getting power values of midplane within domain failed. | An error occurs while the CMM is reading the power values of midplane within domain. |
| Getting power values of mt[*number*] within domain failed.<br>where the *number* represents the specified mt. | An error occurs while the CMM is reading the power values within domain of specified rear LED card. |
| Getting power values of PM Cooling Device *number* failed<br>where the *number* represents the specified PM cooling device. | An error occurs while the CMM is reading the power values of specified power supply cooling device. |
| Getting status of domain *domain_number* failed<br>where *domain_number* identifies the power domain. | An error occurs while the CMM is reading the status of specified domain. |
| Invalid option for this blade: *option*<br>where *option* identifies the unacceptable option. | The user attempts to issue a command with an option which is invalid for the targeted compute node. |
| Maximum CPU Speed not available. | An error occurs while the CMM is reading maximum CPU Speed. |
| pcap must be between *min* and *max* Watts.<br>where *min* and *max* represent the minimum and maximum wattage values permitted. | The user input for power cap is out of the range. |
| Power value is not in the guaranteed capping range. | The user attempts to set a power value that is out of range. |
| The -spl wattage value must be in the range of *lower_limit* and *upper_limit*<br>where *lower_limit* and *upper_limit* indicate the upper and lower wattage range limits. | The user attempts to set a static power limit wattage value that is out of range. |
| The -spl percentage value must convert to a wattage value in the range of *lower_limit* and *upper_limit*<br>where *lower_limit* and *upper_limit* indicate the upper and lower wattage range limits. | The user attempts to set a static power limit percentage value that is outside of the wattage range. |

Table 118. fuelg command errors (continued)

| Error message | Definition |
|---|---|
| The acoustic attenuation setting could not be set because compute nodes in the chassis require more cooling than the selected policy would provide. | The user attempts to set an acoustic attenuation setting that conflicts with chassis cooling requirements. |
| The nebs mode setting could not be set because compute nodes in the chassis require more cooling than the selected policy would provide.<br>**Note:** This error message applies only to CMMs installed in a Lenovo Flex System Carrier-Grade chassis. | The user attempts to select a NEBS mode that exceed the chassis cooling capacity. |
| The Power Management Policy is not applicable when a 1200W or 1400W power module is installed. | The user attempts to select a power management policy that is not compatible with power modules installed in the chassis. |
| There is no air flow trending data to display. | An error occurs while the CMM is reading air flow trending data. |
| There is no thermal trending data to display. | An error occurs while the CMM is reading thermal trending data. |
| There is no trending data to display. | An error occurs while the CMM is reading power trending data. |
| This blade does not support power capping | A user tries to enable power capping for a compute node that does not support this feature. |
| Unable to change power management settings, domain may be oversubscribed. | An error occurs while the CMM is configuring the power management policy. |

## groups command errors

This topic lists errors for the groups command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “groups command” on page 159 for information about command syntax and examples of command use.

Table 119. groups command errors

| Error message | Definition |
|---|---|
| -add and -clear can not be issued together | A user tries to use the -add and -clear options at the same time. |
| -n and -a must be provided for adding/modifying a group | A user tries to add or modify a group without specifying the group name (-n) or role-based security level (-a). |
| -n must be provided for deleting a group | A user tries to delete a group without specifying the group name (-n). |
| Adding/Deleting/Modifying group *group_name* failed where *group_name* is the group name that was entered. | An error occurs while the CMM is adding, deleting, or modifying a group. |
| Error: the RBS permissions capability is not enabled | A user tries to specify RBS permissions when role-based security is not enabled. |
| Getting group *group_name* failed<br>where *group_name* is the group name that was entered. | An error occurs while the CMM is retrieving the group name. |
| Getting groups failed | An error occurs while the CMM is executing the command. |

Table 119. groups command errors (continued)

| Error message | Definition |
|---|---|
| Group *group_name* not found<br>where *group_name* is the group name that was entered. | A user tries to perform an operation on a group name that does not exist. |
| Group name *group_name* already existed<br>where *group_name* is the group name that was entered. | A user tries to enter a group name that already exists. |
| Groups are full, max of *max_num_groups* groups reached<br>where *max_num_groups* is the maximum name number of groups that are allowed. | A user tries to enter more groups than the system supports. |
| Invalid authority level | A user tries to specify an RBS authority level that is not valid. |
| Invalid device number (first number must be smaller): *number*<br>where *number* is the device number that is not valid. | A user tries to specify RBS authority levels using a range of devices that is not valid. |
| Invalid device number: *number*<br>where *number* is the device number that is not valid. | A user tries to specify RBS authority levels without specifying a valid device scope. |
| Invalid rbs device (must be same device): *device*<br>where *device* is the device that is not valid. | A user tries to specify RBS authority levels without specifying a valid device scope. |
| Invalid rbs device: *device*<br>where *device* is the device that is not valid. | A user tries to specify RBS authority levels without specifying a valid device scope. |
| Invalid rbs device: Must specify device number | A user tries to specify RBS authority levels without specifying a valid device scope. |
| Invalid rbs role list | A user tries to specify a list of RBS authority levels that is not valid. |
| Invalid rbs role: *role*<br>where *role* is the authority level that is not valid. | A user tries to specify an RBS authority level that is not valid. |
| Must be set at least one rbs role for this user. | A user tries to set up a group without specifying a role. |
| The group name cannot be longer than *max_length* characters.<br>where *max_length* is the maximum number of characters allowed in a group name. | A user tries to enter a group name that is longer than the maximum length. |

## health command errors

This topic lists errors for the health command.

See "Common errors" on page 407 for a list of error messages that apply to all commands. See "health command" on page 164 for information about command syntax and examples of command use.

Table 120. health command errors

| Error message | Definition |
|---|---|
| -f and -k must be used exclusive of each other.<br>**Note:** This error message applies only to CMMs installed in a Lenovo Flex System Carrier-Grade chassis. | A user tries to issue the -f and -k command options at the same time. |
| Commands cannot be issued to the standby CMM right now. The primary CMM is initializing. Please try again later. | A user tries to issue a command to the standby CMM when it is unavailable. |

*Table 120. health command errors (continued)*

| Error message | Definition |
|---|---|
| Commands cannot be issued to the standby CMM right now. The primary CMM is verifying the code level on the standby CMM. Please try again later. | A user tries to issue a command to the standby CMM when it is unavailable. |
| Commands cannot be issued to the standby CMM right now. The standby CMM is flashing. Please try again later. | A user tries to issue a command to the standby CMM when it is unavailable. |
| Commands cannot be issued to the standby CMM right now. The standby CMM is in an unknown state. Please try again later. | A user tries to issue a command to the standby CMM when it is unavailable. |
| Commands cannot be issued to the standby CMM right now. The standby CMM is in post-flash initialization. Please try again later. | A user tries to issue a command to the standby CMM when it is unavailable. |
| Commands cannot be issued to the standby CMM right now. The standby CMM is not present. Please try again later. | A user tries to issue a command to the standby CMM when it is unavailable. |
| Commands cannot be issued to the standby CMM right now. Please try again later. | A user tries to issue a command to the standby CMM when it is unavailable. |
| Error checking standby CMM status. Commands cannot be issued to the standby CMM right now. | A user tries to issue a command to the standby CMM when it is unavailable. |
| Getting system health summary failed. | An error occurs while the CMM is reading the system health summary. |

## help command errors

This topic lists errors for the help command.

There are no unique errors for the help command. See “Common errors” on page 407 for a list of error messages that apply to all commands. See “help command” on page 171 for information about command syntax and examples of command use.

## history command errors

This topic lists errors for the history command.

There are no unique errors for the history command. See “Common errors” on page 407 for a list of error messages that apply to all commands. See “history command” on page 173 for information about command syntax and examples of command use.

## ifconfig command errors

This topic lists error messages for the ifconfig command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “ifconfig command” on page 174 for information about command syntax and examples of command use.

*Table 121. ifconfig command errors*

| Error message | Definition |
|---|---|
| -d must be set to 'full' when -r is set to '1000auto' | A user tries to set the -r command option to `1000auto` while the -d option is set to other than `full`. |
| -em can't be allowed in this passthru module | The user tries to issue a command with the -em option for an I/O-passthru module that does not support this option. |
| -em cannot be reconfigured while Stacking Mode is enabled on the CMM. | The user tries to issue a command with the -em option while Stacking Mode is enabled on the CMM. |
| -em not supported on switch[*bay*]<br>where *bay* identifies the I/O-bay number. | The user tries to issue a command with the -em option to an I/O module that does not support it. |
| -ep cannot be reconfigured while Stacking Mode is enabled on the CMM. | The user tries to issue a command with the -ep option while Stacking Mode is enabled on the CMM. |
| -ipv6static, -dhcp6, and -sa6 can't all be disabled. | A user tries to issue a command that disables -ipv6static, -dhcp6, and -sa6 at the same time. |
| -pip can't be allowed in this passthru module | The user tries to issue a command with the -pip option to a I/O-passthru module that does not support this option. |
| -pip cannot be reconfigured while Stacking Mode is enabled on the CMM. | The user tries to issue a command with the -pip option while Stacking Mode is enabled on the CMM. |
| -pip not supported on switch[*bay*]<br>where *bay* identifies the I/O-bay number. | The user tries to issue a command with the -pip option to an I/O module that does not support it. |
| -up and -down can not be both used in same command. | The user tries to issue a command with both the -up and -down options. |
| -up and -down cannot be used in the same command. | The user tries to issue a command with both the -up and -down options. |
| -up/down is read-only for blade target | A user tries to enable or disable the Ethernet interface for a compute node. These options are not supported for the compute node command target. |
| An error occurred while reading Protected Mode information. | An error occurs while the CMM is reading the protected mode information. |
| Can't find management NI | An error occurs while attempting to locate the management network interface. |
| Configuration not supported on this I/O Module type. | The user tries to issue a command for the configuration which is not supported by targeted I/O module type. |
| Disabling IP configuration failed. | An error occurs while the CMM is disabling the new IP configuration. |
| Enabling IP configuration failed. | An error occurs while the CMM is enabling the new IP configuration. |
| Error converting the i6 address from string to bytes. | An error occurs while converting the i6 address from a string to bytes. |
| Error parsing NI info: *error_ID*<br>where *error_ID* identifies the error that occurred. | An error occurs while processing network interface information. |
| Error reading data for Link-local address. | An error occurs while the CMM is reading data for the link-local address. |
| Error reading data for Link-local address prefix length. | An error occurs while the CMM is reading data for the link-local address prefix length. |

Table 121. ifconfig command errors (continued)

| Error message | Definition |
|---|---|
| Error reading data for options -id, -i6, -p6, and -g6 | An error occurs while the CMM is reading data for the command options. |
| Error reading data for Stateless auto-config IP Addresses. | An error occurs while the CMM is reading the stateless auto-configuration IP address. |
| Error reading network configuration | An error occurs while reading the network configuration. |
| Error reading NI info | An error occurs while reading network interface information. |
| Error reading the data rate. | An error occurs while the CMM is reading the data rate setting of a network interface (eth0 or eth1). |
| Error validating network interface name. | An error occurs while validating the network interface name. |
| Error validating the ID | An error occurs while validating the ID. |
| Gateway configuration is not allowed on this IO module. | A user tries to configure the gateway for an I/O module that does not support this feature. |
| Getting current active advanced failover mode failed | An error occurs while the CMM is reading the advanced failover mode. |
| I/O Module is in Protected Mode and cannot change its configuration method. | A user tries to change the configuration of an I/O module while it is in protected mode. |
| I/O Module is in Protected Mode and cannot change its IP configuration. | A user tries to change the configuration of an I/O module while it is in protected mode. |
| I/O Module is in Stacking Mode and cannot change its Gateway configuration. | The user tries to issue a command to change the Gateway configuration with the I/O Module in Stacking Mode. |
| I/O Module is in Stacking Mode and cannot change its IP configuration. | The user tries to issue a command to change the IP configuration with the I/O Module in Stacking Mode. |
| I/O Module is in Stacking Mode and cannot change its Subnet configuration. | The user tries to issue a command to change Subnet configuration with I/O Module in Stacking Mode. |
| Include -id only when setting -i6, -p6, or -g6 | The user tries to set a value for -id without specifying an additional command option that is needed. |
| Interface *label* is not configured correctly<br>where *label* identifies the interface. | A user tries to enter incorrect configuration information for the identified interface. |
| Interface *option* is read-only.<br>where *option* identifies the command option | The user tries to configure an option parameter that is read-only. |
| Interface *label* is read-only.<br>where *label* identifies the interface. | A user tries to configure an interface that is read only. |
| Invalid IP arg for *option*: *ip_address*. Each byte has to be in the range (0-255)<br>where:<br>• *option* identifies the command option<br>• *ip_address* identifies the invalid IP address argument | The user tries to enter an IP address that is out of range. IP addresses must follow the standard format: *xxx.xxx.xxx.xxx*, where each *xxx* is a number from 0 to 255. |
| Invalid IP arg for *option*: *ip_address*. Enter 4 bytes separated by 3 dots<br>where:<br>• *option* identifies the command option<br>• *ip_address* identifies the invalid IP address argument | The user tries to enter an IP address that is too long. IP addresses must follow the standard format: *xxx.xxx.xxx.xxx*, where each *xxx* is a number from 0 to 255. |

*Table 121. ifconfig command errors (continued)*

| Error message | Definition |
|---|---|
| Invalid IP arg for *option*: *ip_address*. Too few bytes where:<br>• *option* identifies the command option<br>• *ip_address* identifies the invalid IP address argument | The user tries to enter an IP address with too few bytes. IP addresses must follow the standard format: *xxx.xxx.xxx.xxx*, where each *xxx* is a number from 0 to 255. |
| Invalid IP arg for *option*: *ip_address*. Too many bytes where:<br>• *option* identifies the command option<br>• *ip_address* identifies the invalid IP address argument | The user tries to enter an IP address with too many bytes. IP addresses must follow the standard format: *xxx.xxx.xxx.xxx*, where each *xxx* is a number from 0 to 255. |
| Invalid IPv6 arg for -*option*: *ip_address* where:<br>• *option* identifies the command option<br>• *ip_address* identifies the invalid IPv6 address argument | The user tries to enter an IPv6 address with the wrong format. |
| Invalid MAC arg for *option*: *address*. Invalid syntax where:<br>• *option* identifies the command option<br>• *address* identifies the invalid MAC address argument | The user tries to enter an invalid MAC address. |
| Invalid MAC arg for *option*: *address*. Multicast addresses not allowed where:<br>• *option* identifies the command option<br>• *address* identifies the invalid MAC address argument | The user tries to enter a multicast address. |
| Invalid MAC arg for *option*: *address*. Too few bytes where:<br>• *option* identifies the command option<br>• *address* identifies the invalid MAC address argument | The user tries to enter a MAC address with too few bytes. |
| Invalid MAC arg for *option*: *address*. Too many bytes where:<br>• *option* identifies the command option<br>• *address* identifies the invalid MAC address argument | The user tries to enter a MAC address with too many bytes. |
| Invalid option for the standby CMM: -f | A user tries to set a floating IPv4 IP address for the standby CMM. (The standby CMM does not support floating IP addresses.) |
| Invalid option for the standby CMM: -f6 | A user tries to set a floating IPv6 IP address for the standby CMM. (The standby CMM does not support floating IP addresses.) |
| Invalid option for this Blade: *option*<br>where *option* identifies the command option. | A user tries to enter a command option that is not supported by a compute node. |
| Invalid option for this I/O Module: *option*<br>where *option* identifies the command option. | A user tries to enter a command option that is not supported by an I/O module. |
| IP configuration is not allowed on this IO module. | A user tries to configure the IP address for an I/O module that does not support this feature. |
| Length has to be less than *maximum* characters.<br>where *maximum* is the maximum number of characters | A user tries to input an option argument that exceed the maximum number of characters that are allowed. |
| Only alphanumeric characters, '.', '_' and '-' allowed. No consecutive '.' allowed. | The user tries to enter a domain name that contains invalid characters. Valid characters that can be used in a hostname are letters, numbers, periods ( . ), dashes ( - ), and underscores ( _ ), with no consecutive periods. |

*Table 121. ifconfig command errors (continued)*

| Error message | Definition |
|---|---|
| Only alphanumeric characters, '_' and '-' allowed. | The user tries to enter an hostname that contains invalid characters. Valid characters that can be used in a hostname are letters, numbers, dashes ( - ), and underscores ( _ ). |
| Option *option* has read-only access for the standby CMM.<br>where *option* identifies the command option | A user tries to configure a network setting for the standby CMM that is read only. |
| Option -s has read-only access for the standby CMM. | The user tries to direct a command to that is not supported to the standby CMM. |
| Protected Mode capability does not exist on this I/O module. | A user tries to set or configure a protected mode feature for an I/O module that does not support protected mode. |
| Protected Mode has already been disabled on the CMM for this I/O module. | A user tries to disable protected mode for an I/O module when the protected mode status is already disabled. |
| Protected Mode has already been enabled on the CMM for this I/O module.<br>In order to activate it, you must access the native management interface of the I/O module and activate Protected Mode there. | A user tries to enable protected mode for an I/O module while the protected mode status is still pending. |
| Protected Mode has to be disabled on this I/O module's native management interface first. | A user tries to:<br>• enable protected mode for an I/O module when the protected mode status is already active.<br>• disable protected mode for an I/O module when the protected mode status is attention or active. |
| Re-enabling interface failed. | An error occurs when enabling an interface. |
| Static IPv4 configuration is not allowed when config method is dhcp | The user tries to set one or more static IPv4 configuration parameters (-i, -s, or -g) when the current IPv4 configuration method (-c) is set to DHCP, or if it is being set to DHCP in this command. |
| Subnet mask configuration is not allowed on this IO module. | A user tries to configure the subnet mask for an I/O module that does not support this feature. |
| The current active advanced failover mode is off | A user tries to issue a command to read the standby CMM network configuration when the advanced failover mode is disabled. |
| The ID provided doesn't match any configured addresses | A user tries to change an IP address that has not yet been configured. |
| The standby CMM must be present and advanced failover must be set to noswap before you can set -f. | A user tries to set an IPv4 floating IP address for a standby CMM that is not installed or has the wrong failover setting. |
| The standby CMM must be present and advanced failover must be set to noswap before you can set -f6. | A user tries to set an IPv6 floating IP address for a standby CMM that is not installed or has the wrong failover setting. |
| The standby Management Module address can't be the same as the primary Management Module address. | A user tries to set the IP addresses of the primary and standby CMMs to the same value. |
| This target is no longer supported by the ifconfig command. | The user tries to direct the command to an invalid command target. |

Table 121. ifconfig command errors (continued)

| Error message | Definition |
|---|---|
| When setting i6, -p6, or g6, -id must be included. | A user tries to configure a compute node static IPv6 configuration and does not include the static configuration ID number. |
| You must enable -ep and -em for this I/O module before you can enable -pm on it. | A user tries to enable protected mode for an I/O module before configuring the -ep and -em command options. |

## info command errors

This topic lists error messages for the info command.

See "Common errors" on page 407 for a list of error messages that apply to all commands. See "info command" on page 202 for information about command syntax and examples of command use.

Table 122. info command errors

| Error message | Definition |
|---|---|
| -path not supported on switch[*bay*]<br>where *bay* identifies the I/O-module bay number. | The user tries to issue a command to a path that an I/O module does not support. |
| blade[*x*] doesn't have path information<br>where *x* identifies the compute node. | An error occurs while the CMM is reading the compute node path information. |
| Option: -path cannot be issued to this target | The user tries to use the -path option on a target that does not support it. |
| switch[*x*] doesn't have path information<br>where *x* identifies the I/O module. | An error occurs while the CMM is reading the I/O module path information. |

## iocomp command errors

This topic lists errors for the iocomp command.

See "Common errors" on page 407 for a list of error messages that apply to all commands. See "iocomp command" on page 209 for information about command syntax and examples of command use.

Table 123. iocomp command errors

| Error message | Definition |
|---|---|
| Error reading I/O Compatibility Detail for blade *node_number*<br>where *node_number* identifies the compute node. | An error occurs while the CMM is reading I/O compatibility for targeted compute node. |
| Error reading I/O Compatibility Detail for switch *bay_number*<br>where the *bay_number* identifies the I/O module. | An error occurs while the CMM is reading I/O compatibility for targeted I/O module. |
| ERROR!!! IOM *bay_number* reports incorrect width! sw_width = *sw_width*<br>where<br>• the *bay_number* identifies the I/O module<br>• *sw_width* identifies the invalid width | An error occurs while the CMM is reading I/O compatibility for targeted I/O module. |
| I/O Compatibility Detail of blade *node_number*: unknown<br>where *node_number* identifies the compute node. | An error occurs while the CMM is reading I/O compatibility for the targeted compute node. |

## ldapcfg command errors

This topic lists error messages for the ldapcfg command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “ldapcfg command” on page 211 for information about command syntax and examples of command use.

*Table 124. ldapcfg command errors*

| Error message | Definition |
|---|---|
| -dn is required when -server is set to dns | A user tries to set DNS as the LDAP server discovery method without specifying a search domain (`-dn` option). |
| A Client DN password is configured, client DN must be configured too. | A user tries to issue a command to remove the client DN setting with the client DN password configured. |
| CMM target name is limited to 63 characters. | A user tries to set a CMM target name that is longer than 63 characters. |
| Both password and confirm password must be provided. | A user tries to issue a command without providing both the password and the confirm password. |
| Client DN password mismatch. Please reenter passwords. | A user tries to issue a command with both -p and -cp options, but their arguments do not match. |
| If a Client DN password is configured, client DN must be configured too. | A user tries to issue a command to configure the client DN password while the client DN is not configured. |
| Invalid option argument for -*option*:*argument*. *format* where:<br>• *option* identifies the option<br>• *argument* identifies the invalid argument<br>• *format* identifies the format of argument | A user tries to issue a command with invalid arguments for the options which do not conform to the format specified. |
| Option argument for -*option* exceeds max length (*maximum* characters): *argument*<br>• *option* identifies the option<br>• *maximum* identifies the maximum allowed number of characters<br>• *argument* identifies the argument | A user tries to set a value for the specified option argument that is longer than the maximum allowed number of characters. |
| Port must be numeric and in the range of 1 and 65535 | A user tries to set a port number that is non-numeric or outside the allowed range. |
| When configuring '-bm cc', -cd and -p must be configured too | A user tries to set a binding method of configured credentials without specifying a client distinguished name (`-cd` option) and client password (`-p` option). |
| You are configuring Client DN password, but no Client DN. Please configure a Client DN. | A user tries to issue a command to set Client DN password while the Client DN is not configured. |

## led command errors

This topic lists errors for the led command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “led command ” on page 221 for information about command syntax and examples of command use.

*Table 125. led command errors*

| **Error message** | **Definition** |
|---|---|
| 'blink' is not supported on blade[*node_number*]<br>where *node_number* identifies the compute node. | The targeted compute node does not support the LED blink function. |
| Error setting system LED. | An error occurs while the CMM is configuring the system LED. |
| Error setting -loc for blade[*node_number*]<br>where *node_number* identifies the compute node. | An error occurs while setting identify LED for the targeted compute node. |
| Error setting -loc for switch[*number*]<br>where *number* identifies the I/O-module bay. | An error occurs while setting identify LED for the targeted I/O module. |
| Error getting LED information from device | An error occurs while retrieving LED information. |
| Error turning off information LED | An error occurs while the user is setting the identify LED to off. |
| The chassis location LED cannot be turned off at this time because one or more blades have their location LED active. | A user issues a command to turn off the chassis identify LED under conditions when this is not allowed. |
| The location LED cannot be turned off. The module is not in a state which allows this operation | A user issues a command to turn off a module location LED under conditions when this is not allowed. |

## list command errors

This topic lists error messages for the list command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “list command” on page 224 for information about command syntax and examples of command use.

*Table 126. list command errors*

| **Error message** | **Definition** |
|---|---|
| Error retrieving topology | An error occurs while retrieving the structure of devices installed in a chassis. |

## monalerts command errors

This topic lists errors for the monalerts command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “monalerts command” on page 226 for information about command syntax and examples of command use.

*Table 127. monalerts command errors*

| **Error message** | **Definition** |
|---|---|
| Invalid syntax. -ec is only allowed to be enabled. | A user tries to disable -ec (legacy alerts). |

## ntp command errors

This topic lists error messages for the ntp command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “ntp command” on page 235 for information about command syntax and examples of command use.

*Table 128. ntp command errors*

| **Error message** | **Definition** |
|---|---|
| Configuring NTP settings failed | An error occurs while configuring NTP settings. |
| Getting NTP configuration failed | An error occurs while retrieving NTP configuration information. |
| Invalid value passed to -en flag. Valid values are enable/ disable | The user input for the -*en* option is invalid. |
| NTP not supported on switch *slot*<br>where *slot* indicates the specified I/O-module subslot. | Network time protocol (NTP) is not supported by the specified I/O module subslot. |
| Please set NTP server name or IP address before enabling NTP | The user tries to enable NTP before setting the server name or IP address. |
| Please set NTP server name or IP address before synchronizing the clock | The user tries to synchronize the clock before setting the NTP server name or IP address. |
| Please set NTP update frequency before enabling NTP | The user tries to enable NTP before setting the update frequency. |
| Please set NTP v3 authentication entry before enabling NTP authentication | The user tries to enable NTP authentication before configuring the v3 authentication. |

## permgroups command errors

This topic lists errors for the permgroups command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “permgroups command” on page 238 for information about command syntax and examples of command use.

*Table 129. permgroups command errors*

| **Error message** | **Definition** |
|---|---|
| -n must be provided for clearing a permission group | A user tries to clear a permission group without the -n option. |
| Adding a permission group failed<br>**Note:** This error message might include additional information that provides details about the error, if this additional information is provided by the process or device. | An error occurs while the CMM is adding a permission group. |
| Adding a permission group failed: max group exceeded | A user tries to add a permission group that exceeds the maximum group limit of 128. |
| Both -n and -a must be provided for adding a permission group | A user tries to add a permission group without the -n and -a options. |
| Clearing a permission group failed<br>**Note:** This error message might include additional information that provides details about the error, if this additional information is provided by the process or device. | An error occurs while the CMM is clearing a permission group. |
| Default permission group *group_name* cannot be deleted where *group_name* is the group name that was entered. | A user tries to delete the default permission group. |

*Table 129. permgroups command errors (continued)*

| Error message | Definition |
|---|---|
| Error: the RBS permissions capability is not enabled | A user tries to specify RBS permissions when role-based security is not enabled. |
| Invalid group name. The group name can only contain numbers, letters, dots, underscores, and hyphens. | A user tries to enter a group name that contains invalid characters. Valid characters that can be used in a group name are letters, numbers, periods ( . ), underscores ( _ ), and hyphens ( - ). |
| Getting permission group information failed<br>**Note:** This error message might include additional information that provides details about the error, if this additional information is provided by the process or device. | An error occurs while the CMM is getting permission group information. |
| Getting permission group names failed<br>**Note:** This error message might include additional information that provides details about the error, if this additional information is provided by the process or device. | An error occurs while the CMM is getting permission group names. |
| Invalid authority level | A user tries to specify an RBS authority level that is not valid. |
| Invalid device number (first number must be smaller): *number*<br>where *number* is the device number that is not valid. | A user tries to specify RBS authority levels using a range of devices that is not valid. |
| Invalid device number: *number*<br>where *number* is the device number that is not valid. | A user tries to specify RBS authority levels without specifying a valid device scope. |
| Invalid rbs device (must be same device): *device*<br>where *device* is the device that is not valid. | A user tries to specify RBS authority levels without specifying a valid device scope. |
| Invalid rbs device: *device*<br>where *device* is the device that is not valid. | A user tries to specify RBS authority levels without specifying a valid device scope. |
| Invalid rbs device: Must specify device number | A user tries to specify RBS authority levels without specifying a valid device scope. |
| Invalid rbs role list | A user tries to specify a list of RBS authority levels that is not valid. |
| Invalid rbs role: *role*<br>where *role* is the authority level that is not valid. | A user tries to specify an RBS authority level that is not valid. |
| Modifying a permission group failed<br>**Note:** This error message might include additional information that provides details about the error, if this additional information is provided by the process or device. | An error occurs while the CMM is modifying a permission group. |
| Must be set at least one rbs role for this user. | A user tries to set up a group without specifying a role. |
| Permission group name *group_name* is in use and it cannot be deleted<br>where *group_name* is the group name that was entered. | A user tries to delete a permission group name that is being used. |
| The permission group name cannot be longer than 63 characters | A user tries to set a permission group name that is longer than 63 characters. |

## ping command errors

This topic lists errors for the ping command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “ping command” on page 242 for information about command syntax and examples of command use.

*Table 130. ping command errors*

| Error message | Definition |
|---|---|
| Error reading network configuration | An error occurs while the CMM is reading the network configuration. |
| Index *index* IP address not found<br>where the *index* an IP address in an index table. | The user tries to specify an IP address index number that is not in the index table. |
| Index is greater than the current number of available IP addresses. Please try again. | The user tries to specify an IP address index number that is not in the index table. |
| IP address *ip_address* not found<br>where the *ip_address* identifies the invalid IP address argument. | The user tries to specify an IP address that is not valid. |
| Not supported by this type of I/O module. Type env -h for help on changing targets. | The user tries to issue a command that is not valid for the command target. |
| The I/O module cannot be pinged while the IP config is protected. | The user tries to ping a protected member of an I/O module stack. |
| This command is not available for switches when protected mode is active | A user tries to ping an I/O module that is operating in protected mode. |

## pmpolicy command errors

This topic lists errors for the pmpolicy command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “pmpolicy command” on page 245 for information about command syntax and examples of command use.

*Table 131. pmpolicy command errors*

| Error message | Definition |
|---|---|
| Getting current policy failed. | An error occurs while the CMM is getting the current policy for a domain. |
| Getting valid policies failed. | An error occurs while the CMM is getting the valid policies for power management. |
| Unable to change power management settings, domain may be oversubscribed. | An error occurs when a user attempts to change the power management settings for a power domain that might be oversubscribed. |

## portcfg command errors

This topic lists errors for the portcfg command.

There are no unique errors for the portcfg command. See “Common errors” on page 407 for a list of error messages that apply to all commands. See “portcfg command” on page 247 for information about command syntax and examples of command use.

## ports command errors

This topic lists error messages for the ports command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “ports command” on page 250 for information about command syntax and examples of command use.

*Table 132. ports command errors*

| Error message | Definition |
|---|---|
| A certificate must first be in place before SSL/HTTPS can be enabled. Try rebooting the CMM, or regenerating the CA certificate with the 'sslcfg -gen ca' command. | A user tries to enable SSL or HTTPS without a valid certificate in place. |
| An SSH server key must first be in place before SSH can be enabled. | A user tries to enable SSH before setting up a valid SSH server key. |
| Cannot perform this command right now. The agent is not active | A user tries to direct a command to an agent that is not active.<br>**Note:** This error message applies to only the I/O module target. |
| CMM security policy disallows -cime enable right now. | A user attempts to enable CIM over HTTPS (-cime) when the current security policy setting does not allow it. |
| CMM security policy disallows -ftpe enable right now. | A user attempts to enable FTP (-ftpe) when the current security policy setting does not allow it. |
| CMM security policy disallows -httpse disable (http enable) right now. | A user attempts to disable HTTPS (-httpse) when the current security policy setting does not allow it. |
| CMM security policy disallows -snmp1ae enable right now. | A user attempts to enable SNMPv1 agent state (-snmp1ae) when the current security policy setting does not allow it. |
| CMM security policy disallows -tcme enable right now. | A user attempts to enable TCP command mode (-tcme) when the current security policy setting does not allow it. |
| CMM security policy disallows -telnete enable right now. | A user attempts to enable the Telnet port (-telnete) when the current security policy setting does not allow it. |
| CMM security policy disallows -tftpe enable right now. | A user attempts to enable TFTP (-tftpe) when the current security policy setting does not allow it. |
| Duplicate port number entered. | A user tries to enter a command with a port number that is already in use. |
| Error reading port *number* info<br>where *number* is the port number that was entered. | An error occurs while reading port number information.<br>**Note:** This error message applies to only the I/O module target. |
| Getting open ports failed | An error occurs while the CMM is retrieving informatory about open ports.<br>**Note:** This error message applies to only the I/O module target. |
| Getting policy state failed | An error occurs while the CMM is getting the security policy state. |

Table 132. ports command errors (continued)

| Error message | Definition |
|---|---|
| Invalid parameter. The timeout must be between 0 and 4294967295 seconds. | A user tries to enter a timeout that is outside of the valid range. |
| Invalid port index | A user tries to enter a port index number that is not valid.<br>**Note:** This error message applies to only the I/O module target. |
| Maximum connections can not exceed *max*<br>where *max* is the maximum number of allowed connections. | A user attempts to configure more than the maximum number of allowed connections.<br>**Note:** This error message applies to only the I/O module target. |
| Maximum connections can not exceed 20. | A user attempts to configure more than 20 connections. |
| No valid server certificate is in place for Secure TCP Command Mode. Try rebooting the CMM, or regenerating the CA certificate with the 'sslcfg -gen ca' command. | A user tries to change the state of Secure TCP Command Mode without a valid certificate in place. |
| Port not in use | A user tries to enter a port number that is not in use.<br>**Note:** This error message applies to only the I/O module target. |
| Port number out of range. | A user tries to enter a port number that is outside of the valid range. |
| Resetting all ports to default values failed. | An error occurs while the CMM is resetting all ports to their default values. |
| SNMPv1 support cannot be disabled. It is required for blade communication with the CMM over the CIN. | A user tries to disable SNMPv1 that is required for communications with compute nodes via CIN.<br>**Note:** This error message applies to only the I/O module target. |
| The total number of secure and legacy connections of TCP Command Mode cannot exceed 20 | A user attempted to configure more than 20 TCP Command Mode connections. |
| This I/O module does not support port link state configuration. | A user tries to enter a command for a port link state which not supported by the targeted I/O module.<br>**Note:** This error message applies to only the I/O module target. |
| This I/O module does not support port speed configuration. | A user tries to enter a command for a speed configuration which not supported by the targeted I/O module. |
| This information is not available when protected mode is active | A user tries to access information that is not available when operating in protected mode.<br>**Note:** This error message applies to only the I/O module target. |
| Validating port failed | An error occurs while validating a port.<br>**Note:** This error message applies to only the I/O module target. |
| Warning: Communication with FSM via Secure TCP Command Mode has been disabled. | A user has disabled the Secure TCP command mode. |
| Warning: Communication with FSM via TCP Command Mode has been disabled. | A user has disabled the TCP command mode. |

## power command errors

This topic lists error messages for the power command.

See "Common errors" on page 407 for a list of error messages that apply to all commands. See "power command" on page 264 for information about command syntax and examples of command use.

*Table 133. power command errors*

| Error message | Definition |
|---|---|
| -ap can only be issued to blade target | A user attempts to apply the -ap option to a device other than a compute node. |
| -ap must be 'restore' or 'auto' for blade[*x*]<br>where *x* is the node bay number. | A user tries to enter a -ap command option argument other than `restore` or `auto` for a storage node that requires one of these arguments. |
| -c can only be issued to blade target | A user tries to direct the `power -c` command option to a non-compute node target. |
| -c must be used with -on or -cycle | A user tries to use the -c command option without specifying the -on or -cycle command options. |
| -cycle can only be issued to blade, I/O module or stand-alone server target | A user tries to direct the `power -cycle` command to a command target that does not support it. |
| -d can only be issued to blade or IO module target | A user attempts to apply the -d option to a device other than a compute node or I/O module. |
| -on/-off/-cycle not supported on switch[*x*]<br>where *x* is the I/O-bay number. | A user tries to direct a `power` command option to an I/O module that does not support it. |
| -on/-off/-softoff/-cycle not supported on blade[*x*]<br>where *x* is the node bay number. | A user tries to direct a `power` command option to a compute node that does not support it. |
| -post can only be issued to I/O module target | A user tries to direct the -post option to a non-I/O module target. |
| -post must be used with -state | A user tries to use the -post command option without specifying the -state command option. |
| -sms can only be issued to blade target | A user attempts to issue the -sms command option to a target that is not a compute node. |
| -sms is not supported on blade[*x*]<br>where *x* is the node bay number. | A user attempts to issue the -sms command option to a compute node target that does not support this feature. |
| -softoff can only be issued to blade or stand-alone server target | A user tries to direct the `power -softoff` command to a command target that does not support it. |
| -state can only be issued to blade, I/O module, or stand-alone server target | A user tries to direct the `power -state` command to a command target that does not support it. |
| -wol, -local, -ap, -d and -sms must be used exclusive of the other options | A user attempts to enter multiple command options together that must be used alone. |
| -wol/-local can only be issued to chassis or blade target | A user tries to direct the `power -wol` or `power -local` command to a command target that does not support it. |
| -wol/-local/-sms not supported on blade[*x*]<br>where *x* is the node bay number. | A user tries to direct a `power` command option to a compute node that does not support it. |
| Error retrieving power state for I/O Module *slot*<br>where *slot* is the I/O-module subslot. | An error occurs while retrieving a power state. |

*Table 133. power command errors (continued)*

| Error message | Definition |
|---|---|
| Getting POST results failed | An error occurs while retrieving POST results. |
| Invalid POST results. | The POST results are not valid. |
| Not supported by this type of I/O module. Type env -h for help on changing targets. | A user attempts to apply an option to an I/O module that does not support the option. |
| POST results not complete: *hex_code*<br>where the *hex_code* value varies based on the problem that was encountered. | The POST results are not available. See the documentation that comes with the device that failed to respond correctly to the `power` command for information about the *hex_code* value. |
| Power not supported on this target | A user tries to direct the `power` command to a command target that does not support it. |
| Powering on/off blade failed. | An error occurs while powering the compute node on or off. |
| Powering on/off I/O Module failed. | An error occurs while the CMM is powering the I/O module on or off. |
| Powering on/off network clock failed. | An error occurs while the CMM is powering the network clock on or off. |
| Powering on/off Telco Alarm Panel failed. | An error occurs while the CMM is powering the Telco Alarm Panel on or off. |
| Resetting blade failed. | An error occurs while the CMM is resetting the compute node. |
| Restarting I/O Module failed. | An error occurs while the CMM is restarting the I/O module. |
| Shutting down OS and powering off blade failed. | An error occurs while the CMM is shutting down the operating system and powering off the compute node. |
| SOL not supported on blade[*x*]<br>where *x* is the node bay number. | A user tries to run a `power` command option that starts a SOL (serial over LAN) session on a compute node that does not support SOL. |
| The argument of -d must be in a range of *min* and *max* where *min* and *max* indicate the range of acceptable values. | A user tries to enter an argument for the -d command option that is out of range. |
| The argument of -d must be numeric | A user tries to enter a non-numeric argument for the -d command option. |
| The I/O Module is powering off. | A user tries to power on, power off, or restart a RAID SAS module which is in the process of powering off. |

## pwrprofile command errors

This topic lists errors for the pwrprofile command.

See "Common errors" on page 407 for a list of error messages that apply to all commands. See "pwrprofile command" on page 271 for information about command syntax and examples of command use.

*Table 134. pwrprofile command errors*

| **Error message** | **Definition** |
|---|---|
| -d is required when -f is other than 'daily' | A user does not specify the -d command option when the -f command option is set to a value other than daily. |
| Adding/deleting/modifying group failed: *error*<br>where *error* is:<br>• The group with the name already existed<br>• Max group definitions reached<br>• The group not found<br>• Invalid parameters<br>• Internal error | An error occurs while the CMM is adding, deleting, or modifying a group. |
| Adding/deleting/modifying power schedule failed: *error*<br>where *error* is:<br>• Max power schedules for this target group reached<br>• Max power schedules reached<br>• The power schedule not found<br>• The group not found<br>• Invalid parameters<br>• Internal error | An error occurs while the CMM is adding, deleting, or modifying a power schedule. |
| Bay numbers and/or ranges of bay numbers must be parentheses enclosed | A user tries to specify a bay number, or range of bay numbers, that is not enclosed in parenthesis. |
| Bay type keyword must be followed by set of parentheses enclosing comma delimited bay numbers and/or ranges of bay numbers | A user tries to specify a bay type keyword that is not enclosed in parenthesis or in an improper format. |
| Getting group information failed: *error*<br>where *error* is specific information about the error. | An error occurs while the CMM is getting group information. |
| Getting schedule information of group *group_index* failed: *error*<br>where:<br>• *group_index* is the group index specified.<br>• *error* is specific information about the error. | An error occurs while the CMM is getting group schedule information. |
| Invalid -d for '-f once' | A user tries to enter an invalid value for the -d command option. |
| Invalid -d for '-f weekly' | A user tries to enter an invalid value for the -d command option. |
| Invalid -servers: No parm or invalid keywords | A user tries to specify an argument for -servers that is incomplete or not valid. |
| Invalid -servers for '-key *key*'<br>where *key* is the key specified. | A user tries to specify an argument for -servers that is not valid. |
| Invalid bay number | A user tries to specify a bay number that is not valid. |
| Invalid group/power schedule index: *index*.<br>where *index* is the index specified. | A user tries to specify a non-numeric index. |
| Invalid group/power schedule index: *index*. It is out of range of 1 - *max*<br>where:<br>• *index* is the index specified.<br>• *max* is the highest index number that can be specified. | A user tries to specify an index that is out of range. |

Table 134. pwrprofile command errors (continued)

| Error message | Definition |
|---|---|
| Invalid group/power schedule index. Maximum value is *max*<br>where *max* is the highest index number that can be specified. | A user tries to specify an index that is out of range. |
| Invalid group index: *group_index*<br>where *group_index* is the group index specified. | A user tries to enter an invalid group index, only specifying the '-'. |
| Invalid group index, no index value provided | A user tries to enter an invalid group index, only specifying the '-'. |
| Invalid option argument for -n: *group_name*. Consecutive dots not allowed<br>where *group_name* is the group name specified. | A user tries to enter an invalid group name. |
| Invalid option argument for -n: *group_name*. Only alphanumeric characters and '.', or '_' allowed<br>where *group_name* is the group name specified. | A user tries to enter an invalid group name. |
| Invalid syntax for group index: *group_index*<br>where *group_index* is the group index specified. | A user tries to enter an invalid group index, without specifying the '-' before the index. |
| Invalid syntax for group index, leading '-' is required | A user tries to enter an invalid group index, without specifying the '-' before the index. |
| Invalid time/day/month | A user tries to enter an time, day, or month that is not valid. |
| Invalid year. it must be between *min* - *max*<br>where *min* and *max* specify the allowed range. | A user tries to enter a year that is out of range. |
| Malformed range | A user tries to enter a range of targets using the wrong syntax. |
| Malformed slot:subslot | A user tries to specify a sub-target using the wrong syntax. |
| No -d required for '-f daily | A user tries to enter a value for the -d command option when none is required. |
| Subslot not allowed in range | A user tries to specify a sub-target that is out of range. |
| Subslots only allowed for blades | A user tries to enter a sub-target for targets other than a compute node or storage node. |
| The bays must be in range of 1 and *max*<br>where *max* is the highest bay number that can be specified. | A user tries to enter a bay number that is out of range. |
| The length of group name exceeds max *max* characters<br>where *max* is the highest number of characters that can be used. | A user tries to specify a group name with too many characters. |
| The length of serial number exceeds max *max* characters<br>where *max* is the highest number of characters that can be used. | A user tries to specify a serial number with too many characters. |
| The length of type/model exceeds max *max* characters<br>where *max* is the highest number of characters that can be used. | A user tries to specify a type or model with too many characters. |
| The string of bays can not be greater than *max* chars<br>where *max* is the highest number of characters that can be used. | A user tries to specify a bay string with too many characters. |

*Table 134. pwrprofile command errors (continued)*

| Error message | Definition |
|---|---|
| When changing -key, -servers must also be changed accordingly. | A user tries to change the -key option without changing the -servers option. |
| When modifying a group, the group index must be specified. | A user tries to modify a group without specifying a group index. |
| When modifying a power schedule, -i must be specified. | A user tries to modify a power schedule without specifying the -d command option. |

## read command errors

This topic lists error messages for the read command.

See "Common errors" on page 407 for a list of error messages that apply to all commands. See "read command" on page 280 for information about command syntax and examples of command use.

*Table 135. read command errors*

| Error message | Definition |
|---|---|
| -p must be specified when restoring the configuration settings | A user tries to restore configuration settings without specifying the required passphrase. |
| -u must be specified when restoring the configuration settings | A user tries to restore configuration settings without specifying the required URL. |
| Argument of option -p must be enclosed in quotation marks. | A user tries to enter a passphrase without enclosing it in quotation marks. |
| Error Log Information:<br>*log_filename*<br>where *log_filename* identifies the log file containing error information. | An error occurs during processing with error information contained in the specified log file. |
| Error opening log file | An error occurs while opening the log file. |
| Error restoring configuration. | An error occurs while restoring the CMM configuration. |
| File transfer failed. *error_string*.<br>where *error_string* is specific information about the error. | An error occurs while transferring a file during file upload. |
| File transfer failed abnormally | An error occurs while transferring a file during file upload. |
| Firmware update is in progress. Try again later. | The user tries to restore the CMM configuration from the Lenovo Flex System chassis midplane while the CMM firmware is updating. |
| Incomplete or malformed URL. | The user tries to use an invalid URL. |
| Option argument for -p exceeds max length (31 characters): *passphrase*<br>where *passphrase* is the passphrase that was entered. | A user tries to enter a passphrase that is too long. |
| Passphrase must have at least 6 characters. | A user tries to enter a passphrase that is too short. |
| Please provide a file name at the end of the URL | The user tries to enter a URL without the required file name. |
| Protocol string length exceeds max of 8 | The user tries to enter a protocol string that is too long. |

Table 135. read command errors (continued)

| Error message | Definition |
|---|---|
| There was a problem retrieving the file. | TFTP encounters an error when transferring the configuration file. |
| Update Failed, invalid remote location specified | File upload fails due to the user entering an invalid location. |
| URL Length exceeds max of 256 | The user tries to enter a URL that is too long. |
| URL syntax checking failed | A user tries to enter an invalid URL. |

## remotechassis command errors

This topic lists error messages for the remotechassis command.

See "Common errors" on page 407 for a list of error messages that apply to all commands. See "remotechassis command" on page 285 for information about command syntax and examples of command use.

Table 136. remotechassis command errors

| Error message | Definition |
|---|---|
| Clearing the internal discovered list of MM's failed. | An error occurs while the CMM is clearing the internal discovered list of CMMs. |
| Discovery cannot be run until SLP has been enabled. | The user tries to discover other Lenovo Flex System chassis on the network when SLP is disabled. |
| Error running discovery. | An error occurs while the CMM is running discovery. |
| Getting last discovery time failed. | An error occurs while the CMM is reading last discovery time. |
| Getting the first entry of the internal discovered list of MM's failed. | An error occurs while the CMM is reading the first entry of the internal discovered list of CMMs. |
| Getting the internal discovered list of MM's failed. | An error occurs while the CMM is reading the internal discovered list of CMMs. |
| Unable to read SLP settings. | An error occurs while the CMM is reading SLP settings. |

## reset command errors

This topic lists error messages for the reset command.

See "Common errors" on page 407 for a list of error messages that apply to all commands. See "reset command" on page 289 for information about command syntax and examples of command use.

Table 137. reset command errors

| Error message | Definition |
|---|---|
| -exd not supported on switch[*bay*]<br>where *bay* identifies the I/O-bay number. | The user tries to issue a command with the -exd option to an I/O module that does not support it. |
| -full not supported on switch[*bay*]<br>where *bay* identifies the I/O-bay number. | The user tries to issue a command with the -full option to an I/O module that does not support it. |

Table 137. reset command errors (continued)

| Error message | Definition |
|---|---|
| -sft not supported on blade[x] | The user tries to issue a command with the -sft option to a compute node that does not support it. |
| -std not supported on switch[*bay*]<br>where *bay* identifies the I/O-bay number. | The user tries to issue a command with the -std option to an I/O module that does not support it. |
| blade[x] must be powered on to issue a soft reset | The user tries to reset a compute node that is powered off. |
| BMC reset not supported. | An error occurs when issuing the `reset -T blade[x]:sp` command. |
| Disabling failover failed. | An error occurs while the CMM is disabling failover. |
| Enabling failover failed. | An error occurs while the CMM is enabling failover. |
| Error checking standby CMM status. Commands cannot be issued to the standby CMM right now. | A user tries to issue a command to the standby CMM when it is unavailable. |
| Failed to reset the standby CMM | An error occurs when issuing the `reset -T mm[p] -standby` command. |
| Firmware update is in progress. Try again later. | A user tries to reset the CMM during a firmware update. The error message displays and the CMM does not reset. |
| Power Operations not supported on blade[x] | A user tries to issue the `reset -T blade[x] -sft` command to a compute node that does not support power operations. |
| Rebooting blade failed. | An error occurs while the CMM is rebooting the compute node. |
| Resetting and running standard/extended/full diagnostics for I/O module failed. | An error occurs while the CMM is resetting and running diagnostics for the I/O module. |
| Resetting blade *node_number* with NMI not supported.<br>where the *node_number* identifies the compute node. | A user tries to reset a compute node that does not support non-maskable interrupts (NMI). |
| Resetting blade *node_number* with NMI failed.<br>where the *node_number* identifies the compute node. | An error occurs while the CMM is resetting a compute node with NMI. |
| Resetting I/O module failed. | An error occurs while the CMM is resetting the I/O module. |
| Resetting not supported on blade[*x*]<br>where the *x* identifies the compute node. | A user tries to reset a compute node that does not support the reset command. |
| Resetting not supported on switch[*x*]<br>where the *x* identifies the I/O module. | A user tries to reset an I/O module that does not support the reset command. |
| Restarting CMM failed | An error occurs while restarting the CMM. |
| SOL not supported on blade[x] | A user tries to start an SOL session with a compute node that does not support the SOL feature. |
| There is no backup CMM installed. | A user tries to enable failover on a CMM reset and there is no standby CMM. |
| This command cannot be issued right now. If you still want to reset the primary CMM, please use 'reset -o' to override this warning. | A condition exists that is preventing the CMM from resetting. You can either wait and try the command again or force the CMM to reset immediately using the `reset -o` override option. |

Table 137. reset command errors (continued)

| Error message | Definition |
|---|---|
| This command cannot be issued right now. The primary CMM is initializing, and a reset might result in a failover. If you still want to reset the primary CMM, please use 'reset -o' to override this warning. | A condition exists that is preventing the CMM from resetting. You can either wait and try the command again or force the CMM to reset immediately using the `reset -o` override option. |
| This command cannot be issued right now. The primary CMM is verifying the code level on the standby CMM. Please try again later. | A user tries to reset the primary CMM while it is busy. |
| This command cannot be issued right now. The standby CMM is flashing, and a reset might result in a failover. Please try again later. | A user tries to reset the primary CMM while the standby CMM is unable to support failover. |
| This command cannot be issued right now. The standby CMM is in a post-flash initialization state, and a reset might result in a failover. If you still want to reset the primary CMM, please use 'reset -o' to override this warning. | A user tries to reset the primary CMM while the standby CMM is unable to support failover. |
| This command cannot be issued right now. The standby CMM is in an unknown state, and a reset might result in a failover. If you still want to reset the primary CMM, please use 'reset -o' to override this warning. | A condition exists that is preventing the CMM from resetting. You can either wait and try the command again or force the CMM to reset immediately using the `reset -o` override option. |
| This command cannot be issued right now. There is no standby CMM present. | A user tries to reset the primary CMM when no standby CMM is available to support failover. |

## scale command errors

This topic lists errors for the scale command.

There are no unique errors for the scale command. See “Common errors” on page 407 for a list of error messages that apply to all commands. See “scale command” on page 291 for information about command syntax and examples of command use.

## sddump command errors

This topic lists errors for the sddump command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “sddump command” on page 296 for information about command syntax and examples of command use.

Table 138. sddump command errors

| Error message | Definition |
|---|---|
| Data dump collection is not supported on blade *x*<br>where *x* is the number of the node bay. | The specified data collection is not supported by the specified compute node. |
| Data dump currently in progress. Please try again later | A user tries to direct a command to target while it is busy performing data collection. |
| Error initializing data dump for switch[*x*]<br>where *x* is the I/O-module bay number. | An error occurs during data collection. |
| Error reading data dump status | An error occurs during data collection. |

*Table 138. sddump command errors (continued)*

| Error message | Definition |
|---|---|
| Error reading error string | An error occurs during data collection. |
| Initiate data collection not supported on blade[*x*]<br>where *x* is the number of the node bay. | The CMM is unable to collect the requested data from the specified compute node. |
| Initiate data dump failed | The CMM is unable initiate data collection. |
| Initiate data dump not supported on switch[*x*]<br>where *x* is the I/O-module bay number. | The selected I/O module does not support data collection. |
| Initiate data collection type failed. | The CMM is unable initiate data collection from thecompute node. |
| This command cannot be issued right now. Another data dump is in progress. | The user attempts to initiate data collection for an I/O module where a data collection is already in progress. |

## sdemail command errors

This topic lists errors for the sdemail command.

See "Common errors" on page 407 for a list of error messages that apply to all commands. See "sdemail command" on page 297 for information about command syntax and examples of command use.

*Table 139. sdemail command errors*

| Error message | Definition |
|---|---|
| -to must be specified. | A user tries to send a service data email message without specifying the recipient. |
| Error sending service data email. | An error occurs when the CMM tries to send a service data email message. |
| Invalid email address. | A user tries to enter an email address that is not valid. |
| Invalid input. Email address must be less than 120 characters. | A user tries to enter an email address that is 120 or more characters long. |
| Subject must be enclosed in quotation marks. | A user tries to send a service data email message with a subject option that is not enclosed in quotation marks. |

## security command errors

This topic lists errors for the security command.

See "Common errors" on page 407 for a list of error messages that apply to all commands. See "security command" on page 298 for information about command syntax and examples of command use.

*Table 140. security command errors*

| Error message | Definition |
|---|---|
| Getting security policy failed | An error occurs while getting the security policy. |
| Setting security policy failed | An error occurs while setting the security policy. |

## service command errors

This topic lists errors for the service command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “service command” on page 301 for information about command syntax and examples of command use.

*Table 141. service command errors*

| Error message | Definition |
|---|---|
| Firmware update is in progress. Try again later, or use the -o flag to override this warning. | A user tries to run a command while the CMM is busy. Run the command using the -o command option to override this warning. |
| Getting status of debug with USB key failed. | An error occurs while the CMM is reading the status of debug with a USB key. |
| Invalid option for this blade: -hard". | The user tries to perform a hard restart on a compute node that does not support the hard restart option. |
| Invalid option for this target: - *option*<br>where *option* identifies the illegal command option that was entered. | The user tries to enter a command option for a target that does not support it. |
| Invalid syntax for this target | A user tries to enter a command that is not correct for the specified command target. |
| This command cannot be issued right now. The primary CMM is verifying the code level on the standby CMM. Please try again later. | A user tries to perform a virtual reseat (service-level reset) of the primary CMM while it is busy. |
| This command cannot be issued right now. The primary CMM is verifying the code level on the standby CMM. Please try again later, or use the -o flag to override this warning. | A user tries to perform a virtual reseat (service-level reset) of the primary CMM while it is busy. Run the command using the -o command option to override this warning. |
| This command cannot be issued right now. The standby CMM is flashing, and a reset might result in a failover. Please try again later. | A user tries to perform a virtual reseat (service-level reset) of the primary CMM while the standby CMM is unable to support failover. |
| This command cannot be issued right now. The standby CMM is flashing, and a reset might result in a failover. Please try again later, or use the -o flag to override this warning. | A user tries to perform a virtual reseat (service-level reset) of the primary CMM while the standby CMM is unable to support failover. Run the command using the -o command option to override this warning. |
| This command cannot be issued right now. There is no standby CMM present. | A user tries to perform a virtual reseat (service-level reset) of the primary CMM when no standby CMM is available to support failover. |

## smtp command errors

This topic lists error messages for the smtp command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “smtp command” on page 304 for information about command syntax and examples of command use.

Table 142. smtp command errors

| Error message | Definition |
|---|---|
| Getting SMTP server host name or IP address failed. | An error occurs while the CMM is reading the SMTP server host name or IP address. |
| Invalid host name or ip address. | A user tries to set the SMTP host name or IP address to an invalid value. |
| Setting SMTP email domain name failed. | An error occurs while the CMM is setting an SMTP email domain name. |
| Setting SMTP server name or IP address failed. | An error occurs while the CMM is setting an SMTP server host name or IP address. |
| SMTP email domain name is not set. | A user tries to view the SMTP email domain name when the value is not set. |
| SMTP server host name or IP address is not set. | A user tries to view the SMTP host name or IP address when the values are not set. |

## snmp command errors

This topic lists error messages for the snmp command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “snmp command” on page 306 for information about command syntax and examples of command use.

Table 143. snmp command errors

| Error message | Definition |
|---|---|
| CMM security policy disallows SNMPv1 enable right now | A user tries to enable SNMPv1 when the security policy does not allow it. |
| Config failed. At least one configured community is required to enable SNMPv1 agent, or if SNMPv1 agent is enabled | A user tries to enable SNMPv1 without a configured community, or tries to delete a community that is required by an existing SNMPv1 agent. |
| Config failed. IP addresses of 0.0.0.0 and 0::0 are allowed only when the community is configed as Get or Set access type | A user tries to set an IP address that is restricted by the community access type. |
| Config failed. System contact must be defined to enable SNMPv1 or SNMPv3 agent, or if SNMPv1 or SNMPv3 agent is enabled. | A user tries to enable SNMPv1 or SNMPv3 without a defined system contact, or tries to delete a system contact that is required by an existing SNMPv1 or SNMPv3 agent. |
| Config failed. System location must be defined to enable SNMPv1 or SNMPv3 agent, or if SNMPv1 or SNMPv3 agent is enabled. | A user tries to enable SNMPv1 or SNMPv3 without a defined system location, or tries to delete a system location that is required by an existing SNMPv1 or SNMPv3 agent. |
| Config failed. You defined a community without an IP address or host name. | A user tries to define a community without specifying an IP address or host name. |
| Config failed. You defined a duplicate community name. | A user tries to define a two communities with the same name. |
| Error sanity checking of SNMPv1/v3 configuration | An error occurs while checking the SNMPv1 or SNMPv3 configuration. |

Table 143. snmp command errors (continued)

| Error message | Definition |
|---|---|
| Invalid community name. | A user tries to set a community name to an invalid value. |
| Invalid host name or ip address. | A user tries to set the SNMP host name or IP address to an invalid value. |

## sol command errors

This topic lists error messages for the sol command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “sol command” on page 319 for information about command syntax and examples of command use.

Table 144. sol command errors

| Error message | Definition |
|---|---|
| An error occurred while disabling SOL globally. | An error occurs while the CMM is disabling SOL globally. |
| An error occurred while disabling SOL on that blade. | An error occurs while the CMM is disabling SOL on a compute node. |
| An error occurred while enabling SOL globally. | An error occurs while the CMM is enabling SOL globally. |
| An error occurred while enabling SOL on that blade. | An error occurs while the CMM is enabling SOL on a compute node. |
| An error occurred while reading the global SOL status. | An error occurs while the CMM is reading the global SOL status. |
| An error occurred while reading the SOL accumulate timeout. | An error occurs while the CMM is reading the SOL accumulate timeout. |
| An error occurred while reading the SOL retry count. | An error occurs while the CMM is reading the SOL retry count. |
| An error occurred while reading the SOL retry interval. | An error occurs while the CMM is reading the SOL retry interval. |
| An error occurred while reading the SOL send threshold. | An error occurs while the CMM is reading the SOL send threshold. |
| An error occurred while reading the SOL session status on that blade. | An error occurs while the CMM is reading the SOL session status on a compute node. |
| An error occurred while setting the SOL accumulate timeout. | An error occurs while the CMM is setting the SOL accumulate timeout. |
| An error occurred while setting the SOL blade reset sequence. | An error occurs while the CMM is processing the command. |
| An error occurred while setting the SOL escape sequence. | An error occurs while the CMM is processing the command. |
| An error occurred while setting the SOL retry count. | An error occurs while the CMM is setting the SOL retry count. |
| An error occurred while setting the SOL retry interval. | An error occurs while the CMM is setting the SOL retry interval. |
| An error occurred while setting the SOL send threshold. | An error occurs while the CMM is setting the SOL send threshold. |

*Table 144. sol command errors (continued)*

| Error message | Definition |
|---|---|
| Checking if this blade supports SOL failed. | An error occurs while the CMM is checking if the selected blade supports SOL. |
| Invalid arg for -status. Must be enabled or disabled. | A user tries to enter an invalid argument for the -status command option. |
| Invalid parameter. The accumulate timeout must be between 1 and 251 inclusive. | A user tries to enter an accumulate timeout that is outside of the valid range. |
| Invalid parameter. The retry count must be between 0 and 7, inclusive. | A user tries to enter a retry count that is outside of the valid range. |
| Invalid parameter. The send threshold must be between 1 and 251 inclusive. | A user tries to enter a send threshold that is outside of the valid range. |
| Retry interval range is too large. Setting to 2550. | A user tries to enter a retry interval that is greater than 2550 ms. If the user tries to enter a retry interval greater than 2550 ms, the retry interval will be set to 2550 ms. |
| SOL not supported on blade[*x*]<br>where *x* identifies the compute node. | A user attempts to initiate an SOL session with a compute node that does not support SOL. |
| This blade does not support SOL. | A user tries to issue the SOL command to a compute node that does not support SOL. |

## sshcfg command errors

This topic lists errors for the sshcfg command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “sshcfg command” on page 326 for information about command syntax and examples of command use.

*Table 145. sshcfg command errors*

| Error message | Definition |
|---|---|
| Getting CLI SSH port failed. | An error occurs while the CMM is reading the CLI SSH port. |
| Getting DSA host key failed. | An error occurs while the CMM is reading the DSA host key. |
| Getting host key size failed. | An error occurs while the CMM is reading the host key size. |
| Getting installed key status failed. | An error occurs while the CMM is reading the installed key status. |
| Getting number of SSH public keys installed failed. | An error occurs while the CMM is reading the number of SSH public keys installed. |
| Getting RSA host key failed. | An error occurs while the CMM is reading the RSA host key. |
| When displaying host keys, -hk must be used by itself. | The user tries to issue a command to display the host keys with option -hk. |

## sslcfg command errors

This topic lists errors for the sslcfg command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “sslcfg command” on page 328 for information about command syntax and examples of command use.

*Table 146. sslcfg command errors*

| Error message | Definition |
|---|---|
| -cabu can only be used with -upld and -u | A user tries to import an externally signed LDAP client certificate and CA bundle without specifying the -upld and -u options. |
| -cabu is required when importing a certificate | A user tries to import an externally signed LDAP client certificate and CA bundle without using the -cabu option to specify a URL. |
| -crlx import/download cannot be used with -dnld, -upld, or -tcx import/download | A user tries to import or download a certificate revocation list when specifying -dnld, -upld, or -tcx import/download at the same time. |
| -csa can only be used with -gen ca or -gen ldapsrv | A user tries to issue the -csa option without the -gen option or without providing the ca or ldapsrv argument for the -gen option. |
| -csa must be specified when the mode is comp | A user tries to generate a CA certificate, failing to specify the certificate signing algorithm while the cryptographic mode is set to comp (compatibility with all NIST cipher suites). |
| -dnld cannot be used with -upld, -tcx import/download, or -crlx import/download | A user tries to download an externally signed server certificate and CA bundle when specifying -upld, -tcx import/download, or -crlx import/download at the same time. |
| -dnld or -upld must be with -u specified | A user tries to issue a download certificate signing request or an import certificate command without the -u option. |
| -f can only be used with -dnld cert/csr | A user tries to specify the format of a certificate or certificate signing request without specifying a download. |
| -remove can only be used with -t client | A user tries to issue the -remove option without the -t option or without providing the client argument for the -t option. |
| -tcx import/download cannot be used with -dnld, -upld, or -crlx import/download | A user tries to import or download a trusted certificate when specifying -dnld, -upld, or -crlx import/download at the same time. |
| -u must be provided to download or import a certificate revocation list. | A user tries to issue a download or import trusted certificate revocation list command without the -u option. |
| -u must be provided to import a trusted certificate | A user tries to issue an import trusted certificate command without the -u option. |
| -upld cannot be used with -dnld, -tcx import/download, or -crlx import/download | A user tries to import an externally signed server certificate and CA bundle when specifying -dnld, -tcx import/download, or -crlx import/download at the same time. |

*Table 146. sslcfg command errors (continued)*

| **Error message** | **Definition** |
|---|---|
| Arguments of required options must not be blank | A user tries to enter a required option without its argument. |
| CA certificate regeneration not permitted. The following nodes require an update to the latest blade firmware: *node*<br>where *node* identifies the compute nodes requiring a firmware update. | A user attempts to regenerate a CA certificate when compute node firmware requires an update to support the change. |
| CA generation does not support user inputs | A user tries to generate a CA certificate with options other than -csa. |
| Cannot open file: *filename*<br>where *filename* is the name of the file that was entered for opening. | An error occurs while the CMM is trying to open a file. |
| CLI map failed error = *error*<br>where *error* specifies error. | An error occurs while the CMM is mapping the file to memory. |
| CMM security policy disallows -httpse disable (http enable) right now. | A user tries to disable the SSL server when the CMM security policy is set to secure. |
| Converting DER back to X509 format failed. | An error occurs while the CMM is converting DER back to X509 format. |
| CSR generation for client failed | An error occurs while the CMM is generating a certificate signing request for a client. |
| CSR generation for server failed | An error occurs while the CMM is generating a certificate signing request for a server. |
| Deleting trusted_cert*index* failed<br>where *index* is the number of the selected trusted certificate, between 1 and 4 (inclusive). | A user tries to delete a nonexistent trusted certificate. |
| Downloading *Cert/CA/CSR* to *argument* failed<br>where:<br>• *Cert/CA/CSR* specifies whether the user tried to download a certificate, certificate authority, or certificate signing request.<br>• *argument* identifies the remote location of the item be downloaded from. It must specify a fully qualified filename. | An error occurs while the CMM is downloading a certificate, certificate authority, or certificate signing request. |
| Error deleting LDAP client CA bundle | An error occurs while the CMM is deleting a certificate authority bundle. |
| Error deleting LDAP client certificate | An error occurs while the CMM is deleting an LDAP client certificate. |
| Error: LDAP Client Certificate Doesn't Exist | A user tries to view or download an externally signed LDAP client certificate that does not exist. |
| Error: Requested Certificate Doesn't Exist | A user tries to view an externally signed server certificate or CA bundle that does not exist. |
| Error: unknown certificate | An error occurs because an unknown certificate type is referred to. |
| Exporting *Cert/CSR/CA* failed<br>where *Cert/CSR/CA* specifies whether the user tried to export a certificate, certificate signing request, or certificate authority. | An error occurs while the CMM is exporting a certificate, certificate signing request, or certificate authority. |

*Table 146. sslcfg command errors (continued)*

| Error message | Definition |
|---|---|
| Externally signed SSL server certificate file format must be PEM or DER. | A user tries to import an externally signed server certificate of the wrong file format. |
| Failed - EnableCRLCheck is enabled but no signed crl installed | An error occurs while setting the state for the LDAP client because no signed certificate revocation list is installed. |
| Failed - no trusted certificate installed | An error occurs while setting the state for the LDAP client because no trusted certificate is installed. |
| Failed - Requested file doesn't exist | A user tries to view or download a trusted certificate or certificate revocation list file that does not exist. |
| File format must be PEM or DER. | A user tries to import a trusted certificate or certificate revocation list of the wrong file format. |
| File to be deleted doesn't exist. | A user tries to delete a trusted certificate, certificate revocation list, externally signed client certificate, or CA bundle file that does not exist. |
| File transfer failed. | An error occurs while transferring a file during file upload. |
| File transfer failed abnormally. | An error occurs while transferring a file during file upload. |
| Generate CA failed | An error occurs during CA certificate generation. |
| Generate LDAP server certificate failed | An error occurs during LDAP server certificate generation. |
| Getting SSL Client Certificate status failed. | An error occurs while the CMM is reading the SSL client certificate status. |
| Getting SSL CSR status failed. | An error occurs while the CMM is reading the SSL certificate signing request status. |
| Getting SSL Server Certificate status failed. | An error occurs while the CMM is reading the SSL server certificate status. |
| Getting SSL Server CSR status failed. | An error occurs while the CMM is reading the SSL server certificate signing request status. |
| Importing *url* failed<br>where *url* is the URL that was entered. | An error occurs while importing the indicated URL. |
| Invalid argument for -view | A user tries to issue a command with an invalid argument for the -view option. |
| Invalid SSL target for certificate revocation list: server | A user tries to issue a command for a certificate revocation list with a target of server'. |
| Invalid SSL target for Trusted certificate: server | A user tries to issue a command for a trusted certificate with a target of server'. |
| Invalid URL for -u: *url*<br>where *url* is the URL that was entered. | A user tries to enter a URL that is not valid. |
| Intermediate Root CA bundle file format must be PEM or DER. | A user tries to import a CA bundle of the wrong file format. |
| LDAP Client Certificate File format must be PEM or DER. | A user tries to import an externally signed client certificate of the wrong file format. |
| LDAP server certificate generation does not support user inputs | A user tries to enter information when generating a LDAP server certificate. |

*Table 146. sslcfg command errors (continued)*

| Error message | Definition |
|---|---|
| LDAP Server must use internally signed SLL Server certificate. The following devices prevent use of an externally signed SSL Certificate with LDAP server.<br>*list of nodes*<br>The LDAP sever will use an internally signed SSL certificate until blocking devices are removed (FSP's) or up-dated to latest firmware (IMMv2)<br>where *list of nodes* specifies the devices that prevent use of externally signed SSL certificates. | A user tries to use externally signed SSL certificates on devices configured to restrict their use. |
| Missing required options. | A user tries to issue a command for the SSL configuration without entering all the required options. |
| Mode nist800-131a requires rsa2048sha256 | A user tries to generate a CA certificate using rsa2048sha1 as the signing algorithm while the cryptographic mode is set to nist800-131a. |
| No *Cert/CSR/CA* available.<br>where *Cert/CSR/CA* specifies whether the user specified a certificate, certificate signing request, or certificate authority. | A user tries to issue a command to download a nonexistent certificate, certificate signing request, or certificate authority. |
| No trusted_cert*index* available.<br>where *index* is the number of the selected trusted certificate, between 1 and 4 (inclusive). | A user tries to issue commands to a nonexistent trusted certificate. |
| No valid client certificate is in place. Type 'sslcfg -h' for syntax help of the SSLclient Certificate generation command. | A user tries to issue a command to enable the SSL client without a valid client certificate in place. |
| No valid server certificate is in place. Type 'sslcfg -h' for syntax help of the SSL Server Certificate generation command. | A user tries to issue a command to enable the SSL server without a valid server certificate in place. |
| No valid trusted certificate is in place. Type 'sslcfg -h' for syntax help of the SSL trusted Certificate importing command. | A user tries to issue a command to enable the SSL client without a valid trusted certificate in place. |
| Reading certificate revocation list failed | An error occurs while reading the certificate revocation list. |
| The externally signed LDAP Client certificate doesn't exist. | A user tries to import an externally signed client certificate that does not exist. |
| The externally signed SSL Server certificate doesn't exist. | A user tries to import an externally signed server certificate that does not exist. |
| The following devices prevent use of an externally signed SSL Certificate with LDAP server.<br>*list of nodes*<br>The LDAP sever will use an internally signed SSL certificate until blocking devices are removed (FSP's) or up-dated to latest firmware (IMMv2)<br>where *list of nodes* specifies the devices that prevent use of externally signed SSL certificates. | A user tries to use externally signed SSL certificates on devices configured to restrict their use. |
| The imported file doesn't exist. | A user tries to import a trusted certificate or certificate revocation list that does not exist. |

Table 146. sslcfg command errors (continued)

| Error message | Definition |
|---|---|
| The intermediate root ca bundle is not a valid chain of trust | A user tries to import an intermediate CA bundle that is not trusted. |
| The LDAP Client intermediate root ca certificate bundle doesn't exist. | A user tries to import an intermediate CA bundle that does not exist. |
| The LDAP Client intermediate root ca certificate bundle file format must be PEM or DER. | A user tries to import an intermediate CA bundle of the wrong file format. |
| The LDAP server is now using externally signed SSL certificate as all end point devices firmware reports they can support. | Advisory message indicating that all devices report support of external SSL certificates. |
| The SSL Server intermediate ca certificate bundle doesn't exist. | A user tries to import a CA bundle that does not exist. |
| The SSL Server root ca certificate doesn't exist. | A user tries to import a certificate that does not exist. |
| There was a problem downloading the file | The user does not have the authority for downloading or an error occurs when downloading. |
| There was a problem retrieving the file. | An error occurs while transferring the file. |
| Update Failed, invalid remote location specified | The location specified for update is not valid. |
| URL syntax checking failed | A user tries to enter a URL that is not valid. |
| Viewing -crl1 failed | An error occurs while viewing certificate revocation list 1. |
| Viewing -crl2 failed | An error occurs while viewing certificate revocation list 2. |
| Viewing -crl3 failed | An error occurs while viewing certificate revocation list 3. |
| Viewing -tc1 failed | An error occurs while viewing trusted certificate 1. |
| Viewing -tc2 failed | An error occurs while viewing trusted certificate 2. |
| Viewing -tc3 failed | An error occurs while viewing trusted certificate 3. |
| Viewing CA failed | An error occurs while viewing a certificate authority. |
| Viewing externally signed LDAP client certificate failed | An error occurs while viewing an externally signed LDAP client certificate. |
| Viewing externally signed server certificate failed | An error occurs while viewing an externally signed server certificate. |
| Viewing intermediate CA bundle failed | An error occurs while viewing an intermediate certificate authority bundle. |
| Viewing internally signed server certificate failed | An error occurs while viewing an internally signed server certificate. |
| Writing X509 format certificate to file failed. | An error occurs while the CMM is writing the X509 format certificate to File. |

## syslog command errors

This topic lists errors for the syslog command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “syslog command” on page 346 for information about command syntax and examples of command use.

*Table 147. syslog command errors*

| Error message | Definition |
|---|---|
| -test must be used exclusive of other options | A user tries to run the -test command option at the same time as other command options. |
| Generating test syslog failed | An error occurs while generating the test syslog. |
| Invalid host name or ip address. | A user tries to enter an invalid hostname or ip address. |
| Port number out of range. | A user tries to enter an invalid port number. |

## tcpcmdmode command errors

This topic lists error messages for the tcpcmdmode command.

See "Common errors" on page 407 for a list of error messages that apply to all commands. See "tcpcmdmode command" on page 351 for information about command syntax and examples of command use.

*Table 148. tcpcmdmode command errors*

| Error message | Definition |
|---|---|
| Error changing TCP command mode connection. | An error occurs while the CMM is changing the TCP command mode Connection. |
| Error disabling tcpcmdmode. | An error occurs while the CMM is disabling the TCP command mode. |
| Error enabling TCP command mode. | An error occurs while the CMM is enabling the TCP command mode. |
| Invalid parameter. Input must be numeric. | A user tries to enter a parameter value for the -t (timeout) command option containing non-numeric characters. For example, `tcpcmdmode -t 200m`. |
| Invalid parameter. The timeout must be between 0 and 4294967295 seconds. | A user tries to enter a parameter value for the -t (timeout) command option that is outside of the valid range. |
| Maximum connections can not exceed *maximum*<br>where *maximum* designates the total number of permitted connections. | A user attempted to configure more connections than the maximum number of connections supported. |
| No valid server certificate is in place for Secure TCP Command Mode. Try rebooting the CMM, or regenerating the CA certificate with the 'sslcfg -gen ca' command. | The user issues a command to enable the Secure TCP Command Mode when a valid server certificate is not in place. |
| The total number of secure and legacy connections of TCP Command Mode cannot exceed *maximum*<br>where *maximum* designates the total number of permitted connections. | A user attempted to configure more TCP Command Mode connections than the maximum number of secure and legacy connections supported. |
| Warning: Communication with FSM via Secure TCP Command Mode has been disabled. | A user has disabled the Secure TCP command mode. |
| Warning: Communication with FSM via TCP Command Mode has been disabled. | A user has disabled the TCP command mode. |

## temps command errors

This topic lists errors for the temps command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “temps command” on page 354 for information about command syntax and examples of command use.

Table 149. temps command errors

| Error message | Definition |
|---|---|
| Error getting temperature data from target | An error occurs while retrieving temperature data. |
| Getting power state of blade *node_number* failed. where *node_number* identifies the compute node. | An error occurs while the CMM is reading the power state of the specified compute node. |
| No temperature available for target | A user tries to read temperature data that is not available. |
| Temperature data is not supported on this target | A user tries to read temperature data from a command target that does not support it. |

## trespass command errors

This topic lists error messages for the trespass command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “trespass command” on page 355 for information about command syntax and examples of command use.

Table 150. trespass command errors

| Error message | Definition |
|---|---|
| twe must be enabled to modify the trespassing warning. | The user tries to issue a command to modify the trespassing warning without the -*twe enabled* setting. |
| The trespassing warning must be quote-delimited. | The user tries to enter a trespassing warning that is not enclosed in double-quotation marks. |
| The trespassing warning is greater than 1600 characters. | The user tries to enter a trespassing warning that is longer than 1600 characters. |

## uicfg command errors

The following table lists error messages for the uicfg command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “uicfg command” on page 357 for information about command syntax and examples of command use.

Table 151. uicfg command errors

| Error message | Definition |
|---|---|
| CMM security policy disallows -cim enable right now | An error occurs when the user tries to use -cim enable but the current security policy will not allow it. |
| CMM security policy disallows -cli (telnet) enable right now | An error occurs when the user tries to use -cli (telnet) enable but the current security policy will not allow it. |
| CMM security policy disallows -snmp (v1 agent) enable right now. | An error occurs when the user tries to use -snmp (v1 agent) enable but the current security policy will not allow it. |
| CMM security policy disallows -tcm enable right now. | An error occurs when the user tries to use -tcm enable but the current security policy will not allow it. |

Table 151. uicfg command errors (continued)

| Error message | Definition |
|---|---|
| CMM security policy disallows -web HTTP enable/HTTPS disable right now. | An error occurs when the user tries to use -web HTTP enable/HTTPS disable but the current security policy will not allow it. |
| Enabling SNMPv1/v3 failed. | The SNMPv1/v3 configuration does not meet required criteria. Possible configuration errors include:<br>• A community is configured without an IP address or host name.<br>• A duplicate community name is configured.<br>• At least one configured community is required to enable SNMPv1.<br>• IP address of 0.0.0.0 is allowed only for the first host name in the first community.<br>• IP address of 0.0.0.0 is allowed only when the first community is configured as GET or SET access type.<br>• System contact must be defined to enable SNMPv1/v3.<br>• System location must be defined to enable SNMPv1/v3. |
| Error sanity checking of SNMP configuration. | An error occurs while the CMM is sanity-checking the SNMP configuration. |
| Maximum connections can not exceed *maximum*<br>where *maximum* designates the total number of permitted connections. | A user has attempted to configure more connections than the maximum number of connections supported. |
| No valid server certificate is in place for Secure TCP Command Mode. Try rebooting the CMM, or regenerating the CA certificate with the 'sslcfg -gen ca' command. | The user issues a command to configure the Secure TCP Command Mode when a valid server certificate is not in place. |
| Reading telnet status failed. | An error occurs while the CMM is reading the telnet status. |
| Reading telnet/ssh/snmpv1/snmpv3 status failed. | An error occurs while the CMM is reading the telnet, ssh, snmpv1, or snmpv3 status. |
| The total number of secure and legacy connections of TCP Command Mode cannot exceed *maximum*<br>where *maximum* designates the total number of permitted connections. | A user attempted to configure more TCP Command Mode connections than the maximum number of secure and legacy connections supported. |
| Warning: Communication with FSM via Secure TCP Command Mode has been disabled. | A user has disabled the Secure TCP command mode. |
| Warning: Communication with FSM via TCP Command Mode has been disabled. | A user has disabled the TCP command mode. |

## update command errors

This topic lists error messages for the update command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “update command” on page 361 for information about command syntax and examples of command use.

*Table 152. update command errors*

| Error message | Definition |
|---|---|
| -img is required for this type of switch. | A user tries to update an individual firmware image, for an I/O module that supports update of individual firmware images, without including the -img option. |
| -r must be used with -u to update firmware to CMM and automatically reboot CMM if firmware update succeeds. | A user tries to enter a command with the -r option to update firmware to a primary CMM, but fails to include the -u option. |
| A reset cannot be issued right now. If you still want to reset the primary CMM, please use 'reset -o' to override this warning. | A condition exists that is preventing the CMM from resetting after the update. You can either wait and try the command again or force the CMM to reset immediately using the `reset -o` override option. |
| A reset cannot be issued right now. The primary CMM is initializing, and a reset might result in a failover. If you still want to reset the primary CMM, please use 'reset -o' to override this warning. | A condition exists that is preventing the CMM from resetting after the update. You can either wait and try the command again or force the CMM to reset immediately using the `reset -o` override option. |
| A reset cannot be issued right now. The primary CMM is verifying the code level on the standby CMM. Please try again later. | A user tries to update and reboot the primary CMM while it is busy. |
| A reset cannot be issued right now. The standby CMM is flashing, and a reset might result in a failover. Please try again later. | A user tries to update and reboot the primary CMM while the standby CMM is unable to support failover. |
| A reset cannot be issued right now. The standby CMM is in a post-flash initialization state, and a reset might result in a failover. If you still want to reset the primary CMM, please use 'reset -o' to override this warning. | A user tries to update and reboot the primary CMM while the standby CMM is unable to support failover. |
| A reset cannot be issued right now. The standby CMM is in an unknown state, and a reset might result in a failover. If you still want to reset the primary CMM, please use 'reset -o' to override this warning. | A condition exists that is preventing the CMM from resetting after the update. You can either wait and try the command again or force the CMM to reset immediately using the `reset -o` override option. |
| Cannot perform this command right now. The agent is not active. | A user tries to enter a command while the agent is not active. |
| Commands cannot be issued to the standby CMM right now. The primary CMM is initializing. Please try again later. | A user tries to issue a command to the standby CMM when it is unavailable. |
| Commands cannot be issued to the standby CMM right now. The primary CMM is verifying the code level on the standby CMM. Please try again later. | A user tries to issue a command to the standby CMM when it is unavailable. |
| Commands cannot be issued to the standby CMM right now. The standby CMM is flashing. Please try again later. | A user tries to issue a command to the standby CMM when it is unavailable. |
| Commands cannot be issued to the standby CMM right now. The standby CMM is in an unknown state. Please try again later. | A user tries to issue a command to the standby CMM when it is unavailable. |
| Commands cannot be issued to the standby CMM right now. The standby CMM is in post-flash initialization. Please try again later. | A user tries to issue a command to the standby CMM when it is unavailable. |
| Commands cannot be issued to the standby CMM right now. The standby CMM is not present. Please try again later. | A user tries to issue a command to the standby CMM when it is unavailable. |

Table 152. update command errors (continued)

| Error message | Definition |
|---|---|
| Commands cannot be issued to the standby CMM right now. Please try again later. | A user tries to issue a command to the standby CMM when it is unavailable. |
| Disabling failover failed. | An error occurs while the CMM is turning off the automatic failover feature. |
| Error checking standby CMM status. Commands cannot be issued to the standby CMM right now. | A user tries to issue a command to the standby CMM when it is unavailable. |
| Error checking standby CMM status. The standby CMM might take over as primary during this reboot. | A user tries to issue a command to the standby CMM that includes the -r flag, when the standby CMM isn't synchronized and running. |
| Error reading information for firmware image *index*. *maximum*<br>where *index* specifies the firmware image. | An error occurs while the CMM is reading information for a specified firmware image. |
| Error reading the number of firmware images. | An error occurs while the CMM is reading the number of firmware images. |
| Flash operation failed. | An error occurs during the flash firmware update. |
| Flash operation failed status *percentage*<br>where the *percentage* value varies based on when the problem was encountered. | An error occurs during the flash firmware update. |
| Flash operation not in process or status unavailable. | An error occurs during the flash firmware update. |
| Flash operation timed out *percentage*.<br>where the *percentage* value varies based on when the problem was encountered. | An error occurs during the flash firmware update. |
| Flash preparation - error sending packet file *filename*.<br>where *filename* identifies the file being updated. | An error occurs during the flash firmware update. |
| Flash preparation error. Packet percent complete *percentage*. Flash percent complete *percentage*.<br>where the *percentage* value varies based on when the problem was encountered. | An error occurs during the flash firmware update. |
| Flash preparation error. Timeout on packet preparation operation *percentage*.<br>where the *percentage* value varies based on when the problem was encountered. | An error occurs during the flash firmware update. |
| Flashing not supported on this target. | A user attempts to run the update command on a module that does not support flash firmware updates. |
| Getting data encryption setting failed. If data encryption is enabled and you are updating the firmware to a level which does not support data encryption, you will lose all your configuration settings as a result. | An error occurs while the CMM is reading the data encryption setting. |
| Getting name of mm *bay_number* failed.<br>where the *bay_number* identifies the CMM specified. | An error occurs while the CMM is reading the name of the CMM in designated bay. |
| Invalid image index. Index must be less than *maximum*<br>where *maximum* designates the largest permitted index value. | A user tries to enter an image index that is greater than the maximum permitted index value. |

*Table 152. update command errors (continued)*

| Error message | Definition |
|---|---|
| Invalid option. | An invalid command option is entered. For the update command, invalid command option errors include:<br>• the -i (IP address) command option does not have an IP address parameter<br>• the -i (IP address) command option specifies an invalid IP address<br>• attempting to enter the -i (IP address) command option without the -n (filename) command option<br>• the -n (filename) command option does not have a file name parameter<br>• attempting to enter the -n (filename) command option without the -i (IP address) command option<br>• attempting to enter the -v (verbose) command option without the -i (IP address) command option and -n (filename) command option<br>• attempting to enter the -v (verbose) command option with the -a command option |
| Invalid syntax. | The user tries to execute a command without specifying a command option. |
| CMM*bay_number* is not installed.<br>where the *bay_number* identifies the CMM specified. | The command is targeted to a CMM bay where no CMM is installed. |
| Rebooting CMM failed. | An error occurs while the CMM is trying to reboot. |
| Status: Unable to read status. | An error occurs while the CMM is reading status. |
| TFTP Error: *error_code*.<br>where the *error_code* can have one of the following values:<br>• Access violation.<br>• Connection failure.<br>• Disk full or allocation exceeded.<br>• File already exists.<br>• File error.<br>• File not found.<br>• Illegal option negotiation.<br>• Illegal TFTP operation.<br>• Unable to allocate memory.<br>• Unknown transfer ID.<br>• Unknown user. | An error occurs when the user attempts to set up the TFTP connection. |
| The primary CMM is initializing. The standby CMM might take over as primary during this reboot. | A user tries to issue a command to the standby CMM that includes the -r flag, when the standby CMM isn't synchronized and running. |
| The primary CMM is verifying the code level on the standby CMM. The standby CMM might take over as primary during this reboot. | A user tries to issue a command to the standby CMM that includes the -r flag, when the standby CMM isn't synchronized and running. |
| The standby CMM is flashing. The standby CMM might take over as primary during this reboot. | A user tries to issue a command to the standby CMM that includes the -r flag, when the standby CMM isn't synchronized and running. |
| The standby CMM is in an unknown state. The standby CMM might take over as primary during this reboot. | A user tries to issue a command to the standby CMM that includes the -r flag, when the standby CMM isn't synchronized and running. |

Table 152. update command errors (continued)

| Error message | Definition |
|---|---|
| The standby CMM is in post-flash initialization. The standby CMM might take over as primary during this reboot. | A user tries to issue a command to the standby CMM that includes the -r flag, when the standby CMM isn't synchronized and running. |
| The standby CMM might take over as primary during this reboot. | A user tries to issue a command to the standby CMM that includes the -r flag, when the standby CMM isn't synchronized and running. |
| There was a problem retrieving the file. | An error occurred when transferring the file. |
| Unable to read blade server VPD bay *bay_numbername*.<br>where the *bay_number* and *name* identify the blade server by location and name. | The command specifies an empty compute node bay or an error occurs when reading the VPD. |
| Unable to read I/O Module VPD bay *bay_numbername*.<br>where the *bay_number* and *name* identify the I/O module by location and name. | The command specifies an empty I/O-bay or an error occurs when reading the VPD. |
| Unable to read MM VPD bay *bay_numbername*.<br>where the *bay_number* and *name* identify the CMM by location and name. | The command specifies an empty CMM bay or an error occurs when reading the VPD. |
| Unable to read VPD for Blade *node_numbername*.<br>where the *node_number* and *name* identify the compute node by location and name. | An error occurs while the CMM is reading the VPD of the targeted compute node. |
| Unknown device type. | The command is targeted to an unknown device type. |
| Update error. Invalid destination. | A user tries to issue a command to a target that is not valid. |

## uplink command errors

This topic lists error messages for the uplink command.

See "Common errors" on page 407 for a list of error messages that apply to all commands. See "uplink command" on page 368 for information about command syntax and examples of command use.

Table 153. uplink command errors

| Error message | Definition |
|---|---|
| -ip must be a valid IP address before enabling -el | A user tries to issue a command to enable the -el without a valid -ip setting. |
| A non-zero IP address must be set before enabling -el. | A user tries to enable -el while both -ip and -ip6 are zero. |
| At least one IP address must be non-zero when -el is enabled. | A user tries to set both -ip and -ip6 to zero while -el is enabled. |
| Both IP addresses must be non-zero for -alert to take effect. | A user sets the alert policy for logical link loss when at least one of the IP address is all zeros and IPv6 is enabled. Even though the alert policy has been set, it will have no effect, due to the all-zero IP address.<br>**Note:** This is not an error message. It is an advisory message informing the user that they have configured an option that will have no effect, based on other command option settings. |

Table 153. uplink command errors (continued)

| Error message | Definition |
|---|---|
| Both IP addresses must be non-zero and IPv6 must be enabled using the ifconfig command for -alert to take effect. | A user sets the alert policy for logical link loss when at least one of the IP address is all zeros and IPv6 is disabled. Even though the alert policy has been set, it will have no effect, due to the all-zero IP address and IPv6 being disabled.<br>**Note:** This is not an error message. It is an advisory message informing the user that they have configured an option that will have no effect, based on other command option settings. |
| Error checking standby CMM status. Commands cannot be issued to the standby CMM right now. | A user tries to issue a command to the standby CMM when it is unavailable. |
| Error converting the IPv6 address from string to bytes. | An error occurs while converting the IPv6 address from a string to bytes. |
| Getting status of failver on Lose/Logical of Physical Link failed. | An error occurs while the CMM is reading status of failver on Lose/Logical of Physical Link. |
| Invalid uplink delay value. | A user tries to enter a delay value that is less than 1 or greater than 255. For example, `uplink -del 0`. |
| No option argument for *option*<br>where *option* is the command option for which no argument was specified. | A user tries to enter a command option without its required argument. |
| The option argument for *option* is out of the valid range (between 1 and 2880 minutes).<br>where *option* is the number of minutes specified. | The user input for an option is out of the range. |
| The option argument for *option* is out of the valid range (between 10 and 172800 seconds).<br>where *option* is the number of seconds specified. | The user input for an option is out of the range. |

## users command errors

This topic lists error messages for the users command.

See "Common errors" on page 407 for a list of error messages that apply to all commands. See "users command" on page 372 for information about command syntax and examples of command use.

Table 154. users command errors

| Error message | Definition |
|---|---|
| -add, -n, -kf and -key must be provided for adding a key to a user and must not be used with other options. | A user tries to add a key to a user profile without the -n, -kf, and -key options, or with other options. |
| -add, -n, -p, -g and -ms must be provided for adding a user and must not be used with other options. | A user tries to add a user profile without the -n, -p, -g, and -ms options, or with other options. |
| -ki must be provided for updating a key | A user tries to update a key without the -ki option. |
| -n, -kf, -upld, -u and/or -ki must be provided for uploading a public key | A user tries to upload a public key without the -n -kf, -upld, -u, and -ki options. |
| -n, -ki, -kf, -dnld and -u must be provided for downloading a public key | A user tries to download a public key without the -n, -ki, -kf, -dnld, and -u options. |

*Table 154. users command errors (continued)*

| Error message | Definition |
|---|---|
| -n and -ki must be provided for removing a key | A user tries to remove a key without the -n and -ki options. |
| -n must be provided for deleting a user | A user tries to delete a user profile without the -n option. |
| -n must be provided for disable a user | A user tries to disable a user profile without the -n option. |
| -n must be provided for enable a user | A user tries to enable a user profile without the -n option. |
| -n must be provided for modify a user | A user tries to modify a user profile without the -n option. |
| -n must be provided for modifying a user, a key, SNMPv3 or centralized management of IPMI/SNMPv3 accounts configuration | A user tries to modify a user profile, a key, SNMPv3, or the centralized management of IPMI/SNMPv3 accounts configuration without the -n option. |
| -n must be provided for unlock a user | A user tries to unlock a user profile without the -n option. |
| -p and -op must be specified when changing your own password. | A user tries to change their own user password without the -n and -op options. |
| Adding an SSH public key to RECOVERY_ID is forbidden | A user tries to add an SSH public key to the RECOVERY_ ID account. |
| Adding a user failed<br>**Note:** This error message might include additional information that provides details about the error, if this additional information is provided by the process or device. | An error occurs while the CMM is adding a user. |
| Both -kf and -key must be provided for updating a key | A user tries to update a key without the -kf and -key options. |
| Deleting a user failed<br>**Note:** This error message might include additional information that provides details about the error, if this additional information is provided by the process or device. | An error occurs while the CMM is deleting a user. |
| Deleting SNMPv3/IPMI user provisioning for *user* failed where *user* is the user name specified by the user<br>**Note:** This error message might include additional information that provides details about the error, if this additional information is provided by the process or device. | An error occurs while the CMM is deleting SNMPv3/IPMI user provisioning.<br>**Note:** Disabling centralized IPMI and SNMPv3 management (provisioning) of a user account deletes the centrally managed user account. If there is a corresponding local account for this user on the CMM, it will remain functional. |
| Disable a user failed<br>**Note:** This error message might include additional information that provides details about the error, if this additional information is provided by the process or device. | An error occurs while the CMM is disabling a user. |
| Deleting public key(s) failed | An error occurs while the CMM is deleting one or more public keys. |
| Downloading to *URL* failed<br>where *URL* is the URL specified by the user | An error occurs when the user tries to download to a specified URL. |
| Duplicate group name: *group_name*<br>where *group_name* is the group name specified by the user | A user tries to create a group name that already exists. |

*Table 154. users command errors (continued)*

| Error message | Definition |
|---|---|
| Enable a user failed<br>**Note:** This error message might include additional information that provides details about the error, if this additional information is provided by the process or device. | An error occurs while the CMM is enabling a user. |
| Error writing data for option -ipmisnmpv3<br>**Note:** This error message might include additional information which provides details about the error and corrective actions. | An error occurs while the CMM is writing IPMIv3 information for the indicated user.<br>**Example:**<br>`system> users -T mm[2] -n test -ipmisnmpv3 enabled`<br>**Error writing data for option -ipmisnmpv3**<br>**User test: account is locked, password must be changed.**<br>**system>**<br>This indicates that the `test` user account is locked and that its password needs to be changed. |
| Export public key failed | An error occurs while the CMM is exporting a public key. |
| Getting public key detail failed | An error occurs while the CMM is getting public key details. |
| Getting user active sessions failed | An error occurs while the CMM is getting user active sessions. |
| Getting user information failed<br>**Note:** This error message might include additional information that provides details about the error, if this additional information is provided by the process or device. | An error occurs while the CMM is getting user information. |
| Getting user names failed<br>**Note:** This error message might include additional information that provides details about the error, if this additional information is provided by the process or device. | An error occurs while the CMM is getting user names. |
| Getting user SSH public key status failed | An error occurs while the CMM is getting user SSH public key status. |
| Group *group_name* not found<br>where *group_name* is the group name specified by the user | An error occurs while the CMM is getting group name. |
| Importing public key failed | An error occurs while the CMM is importing a public key. |
| Index can not be 'all' for updating a key | A user tries to update a key for all users. |
| Index can not be 'all' with -dnld | A user tries to download a public user key, specifying it for all keys. |
| Index can not be 'all' with -e | A user tries to display the entire key for all keys. |
| Index can not be 'all' with -upld. | A user tries to upload all public user keys in a single command. |
| Invalid username. The username can only contain numbers, letters, dots, and underscores. | A user tries to enter a user name that contains invalid characters. Valid characters that can be used in a group name are letters, numbers, periods ( . ), and underscores ( _ ). |

*Table 154. users command errors (continued)*

| Error message | Definition |
|---|---|
| Modifying user failed<br>**Note:** This error message might include additional information that provides details about the error, if this additional information is provided by the process or device. | An error occurs while the CMM is modifying a user. |
| Modifying user password failed<br>**Note:** This error message might include additional information that provides details about the error, if this additional information is provided by the process or device. | An error occurs while the CMM is modifying a user password. |
| No '-ki' required for adding a key to user | A user tries to add a key to a user profile with the -ki option. |
| No key index *key_index* found for user: *user_name*<br>where *key_index* is the is a user profile index key and *user_name* is a user name | A user tries to access a key index that has not been set for the specified user. |
| One default permission group, or one or more custom groups can be specified | A user tries to set up the wrong number or type of permission group. |
| Password must have at least a number and a letter | A user tries to set a user password that does not contain at least one letter and one number. |
| Please provide a target for account management by CMM: -prov_target (iom, node, all) | A user tries to modify the user account management state ("-am" option) or the centralized management of IPMI/ SNMPv3 accounts configuration ("-ipmisnmpv3" option) without specifying the -prov_target option. |
| The argument of option -af contains invalid characters. Only alphanumeric, comma, asterisk, question mark, hyphen, period, colon, percent, and exclamation point characters are valid. | A user tries to enter host information that contains invalid characters. Valid characters that can be used for host information are letters, numbers, commas ( , ), asterisk ( * ), question mark ( ? ), hyphen ( - ), period ( . ), colon ( : ), percent sign ( % ), and exclamation point ( ! ). |
| The argument of option -af length can not be greater than 512. | A user tries to set host information that is greater than or equal to 512 characters. |
| The argument of option -af must start with 'from=' | A user tries to set host information without starting the string with "from=". |
| The argument of option -cm must be enclosed in quotation marks. | A user tries to specify a comment without enclosing the string in double-quotation marks. |
| The argument of option -key must be enclosed in quotation marks. | A user tries to specify a key name without enclosing the string in double-quotation marks. |
| The argument of option -ki must be numeric or 'all' | A user tries to specify an argument for the -ki command option other than a key number, between 1 and 20, or all. |
| The length of group names exceeds max of *maximum*<br>where *maximum* is the maximum group name length specified by the user | A user tries to set a group name length that is too long. |
| The length of the group name of *group_name* exceeds max of *maximum*<br>where *group_name* is the is group name entered and *maximum* is the maximum group name length specified by the user | A user tries to set a group name that exceeds the maximum number of characters. |

Table 154. users command errors (continued)

| Error message | Definition |
|---|---|
| The max sessions can not be greater than 20 | A user tries to set a maximum number of user sessions that is greater than 20. |
| The number of groups exceeds max of *maximum*<br>where *maximum* is the maximum number of groups specified by the user | A user tries to set up too many groups. |
| The user name cannot be longer than *maximum* characters for SNMPv3/IPMI provisioning.<br>where *maximum* is the maximum number of characters allowed | A user tries to set a user name that is longer than the maximum numbers of characters specified for SNMPv3 or IPMI provisioning. |
| The user name can not be longer than 32 characters. | A user tries to set a user name that is longer than 32 characters. |
| The user password must be in range of 5 and 32 | A user tries to set a user password that is less than 5 characters or longer than 32 characters. |
| There was a problem downloading the file | The user does not have the authority for downloading or an error occurs when downloading. |
| There was a problem retrieving the file. | An error occurred when transferring the file. |
| Unlock a user failed<br>**Note:** This error message might include additional information that provides details about the error, if this additional information is provided by the process or device. | An error occurs while the CMM is unlocking a user. |
| Updating public key failed<br>**Note:** This error message might include additional information that provides details about the error, if this additional information is provided by the process or device. | An error occurs while the CMM is updating a public key. |
| User must be added before adding a key to it. | A user tries to add a key to a user profile that does not exist. |
| User with supervisor role can not be disabled | An error occurs when one user tries to disable another user that has a supervisor role. |
| New User Creation Method cannot be changed: SMTP server not configured | An error occurs when user attempts to switch new user creation method from username&password to username&email without properly setting SMTP server first. |

## vlan command errors

This topic lists error messages for the vlan command.

See “Common errors” on page 407 for a list of error messages that apply to all commands. See “vlan command” on page 391 for information about command syntax and examples of command use.

*Table 155. vlan command errors*

| Error message | Definition |
|---|---|
| -sol must be enabled on one vlan | A user attempts to disable SOL when only one VLAN is in use. |
| All changes must be committed using -commit before the commit timeout expires. | A user fails to commit CMM changes within the specified time period. |
| All changes must be committed within *time* minutes using -commit.<br>where *time* is the commit time limit. | A user fails to commit CMM changes within the specified time period. |
| Cannot enable VLAN - configuration incomplete. | A user attempts to enable a VLAN entry before configuring all required fields. |
| Changes to the VLAN ID and IP config will take affect after the entry is enabled or restarted. | Advisory message indicating that additional user action is required before a change takes effect. |
| Error writing -i - the IP address is either a duplicate, or in the same subnet as another entry | A user attempts to enter a duplicate IPv4 IP address. |
| Error writing -i6 - the IP address is either a duplicate, or in the same subnet as another entry | A user attempts to enter a duplicate IPv6 IP address. |
| Error writing -sol - currently assigned to another VLAN. | A user attempts to enable the -sol option for a VLAN entry before disabling the option on another VLAN entry where it is already in use. |
| Error writing -vid - the VLAN ID is a duplicate. | A user attempts to enter a duplicate VLAN ID. |
| Invalid syntax. -c cannot be used on the fixed entry. | A user attempts to set the IPv4 configuration method of the first CMM VLAN index entry (referred to as the fixed entry), that can not be changed. |
| Invalid syntax. -c6 cannot be used on the fixed entry. | A user attempts to set the IPv6 configuration method of the first CMM VLAN index entry (referred to as the fixed entry), that can not be changed. |
| Invalid syntax. -commit must be used by itself. | A user attempts to issue a command to the CMM with the -commit option while specifying another argument or option. |
| Invalid syntax. -cto must be used by itself. | A user attempts to issue a command to the CMM with the -cto option while specifying another argument or option. |
| Invalid syntax. -delete must be used by itself, or in combination with -vi. | A user attempts to issue a command to the CMM with the -delete option while specifying another argument or option, other than the -vi option. |
| Invalid syntax. -g cannot be used on the fixed entry. | A user attempts to set the IPv4 gateway of the first CMM VLAN index entry (referred to as the fixed entry), that can not be changed. |
| Invalid syntax. -g6 cannot be used on the fixed entry. | A user attempts to set the IPv6 gateway of the first CMM VLAN index entry (referred to as the fixed entry), that can not be changed. |
| Invalid syntax. -i cannot be used on the fixed entry. | A user attempts to set the IPv4 address of the first CMM VLAN index entry (referred to as the fixed entry), that can not be changed. |
| Invalid syntax. -i6 cannot be used on the fixed entry. | A user attempts to set the IPv6 address of the first CMM VLAN index entry (referred to as the fixed entry), that can not be changed. |

*Table 155. vlan command errors (continued)*

| Error message | Definition |
|---|---|
| Invalid syntax. -p6 cannot be used on the fixed entry. | A user attempts to set the IPv6 prefix length of the first CMM VLAN index entry (referred to as the fixed entry), that can not be changed. |
| Invalid syntax. -s cannot be used on the fixed entry. | A user attempts to set the IPv4 subnet of the first CMM VLAN index entry (referred to as the fixed entry), that can not be changed. |
| Invalid syntax. -sm1 cannot be used on the fixed entry. | A user attempts to set an IPv4 subnet mask of the first CMM VLAN index entry (referred to as the fixed entry), that can not be changed. |
| Invalid syntax. -sm2 cannot be used on the fixed entry. | A user attempts to set an IPv4 subnet mask of the first CMM VLAN index entry (referred to as the fixed entry), that can not be changed. |
| Invalid syntax. -sm3 cannot be used on the fixed entry. | A user attempts to set an IPv4 subnet mask of the first CMM VLAN index entry (referred to as the fixed entry), that can not be changed. |
| Invalid syntax. -sp61 cannot be used on the fixed entry. | A user attempts to set an IPv6 subnet prefix length of the first CMM VLAN index entry (referred to as the fixed entry), that can not be changed. |
| Invalid syntax. -sp62 cannot be used on the fixed entry. | A user attempts to set an IPv6 subnet prefix length of the first CMM VLAN index entry (referred to as the fixed entry), that can not be changed. |
| Invalid syntax. -sp63 cannot be used on the fixed entry. | A user attempts to set an IPv6 subnet prefix length of the first CMM VLAN index entry (referred to as the fixed entry), that can not be changed. |
| Invalid syntax. -sr1 cannot be used on the fixed entry. | A user attempts to set an IPv4 subnet route of the first CMM VLAN index entry (referred to as the fixed entry), that can not be changed. |
| Invalid syntax. -sr2 cannot be used on the fixed entry. | A user attempts to set an IPv4 subnet route of the first CMM VLAN index entry (referred to as the fixed entry), that can not be changed. |
| Invalid syntax. -sr3 cannot be used on the fixed entry. | A user attempts to set an IPv4 subnet route of the first CMM VLAN index entry (referred to as the fixed entry), that can not be changed. |
| Invalid syntax. -sr61 cannot be used on the fixed entry. | A user attempts to set an IPv6 subnet route of the first CMM VLAN index entry (referred to as the fixed entry), that can not be changed. |
| Invalid syntax. -sr62 cannot be used on the fixed entry. | A user attempts to set an IPv6 subnet route of the first CMM VLAN index entry (referred to as the fixed entry), that can not be changed. |
| Invalid syntax. -sr63 cannot be used on the fixed entry. | A user attempts to set an IPv6 subnet route of the first CMM VLAN index entry (referred to as the fixed entry), that can not be changed. |
| Invalid syntax. -state cannot be used on the fixed entry. | A user attempts to set the VLAN state of the first CMM VLAN index entry (referred to as the fixed entry), that can not be changed. |

Table 155. vlan command errors (continued)

| Error message | Definition |
|---|---|
| Invalid syntax. -tag cannot be used on non-default entries. | A user attempts to enable or disable the VLAN tagging state of the first CMM VLAN index entry (referred to as the fixed entry), that can not be changed. |
| Invalid syntax. -vi is needed to perform this operation. | A user attempts to add or modify a CMM VLAN entry without specifying the VLAN entry index number. |
| Invalid syntax. -vid is needed to create a new entry. | A user attempts to create a new entry without specifying a VLAN ID. |
| Invalid syntax. restart can only be used on individual, non-fixed entries. | A user attempts to restart the first CMM VLAN index entry (referred to as the fixed entry), that can not be restarted. |
| Invalid syntax. The fixed entry cannot be deleted. | A user attempts to delete the first CMM VLAN index entry (referred to as the fixed entry). This entry can not be deleted. |

## volts command errors

This topic lists errors for the volts command.

See "Common errors" on page 407 for a list of error messages that apply to all commands. See "volts command" on page 403 for information about command syntax and examples of command use.

Table 156. volts command errors

| Error message | Definition |
|---|---|
| Error getting voltage data from target | An error occurs while retrieving voltage data. |
| Getting power state of blade *node_number* failed.<br>where *node_number* identifies the compute node. | An error occurs while the CMM is reading the power state of the targeted compute node. |
| No voltage data available for target | A user tries to read voltage data that is not available. |
| Voltage data is not supported on this target | A user tries to read voltage data from a command target that does not support it. |

## write command errors

This topic lists error messages for the write command.

See "Common errors" on page 407 for a list of error messages that apply to all commands. See "write command" on page 404 for information about command syntax and examples of command use.

Table 157. write command errors

| Error message | Definition |
|---|---|
| Argument of option -p must be enclosed in quotation marks. | A user tries to enter a passphrase without enclosing it in quotation marks. |
| Error generating configuration. | The CMM is unable to generate the configuration. |
| Error receiving the backup file. | An error occurs during backup file processing. |
| File transfer failed. *error_string*.<br>where *error_string* is specific information about the error. | The CMM is unable to transfer the file. |

Table 157. write command errors (continued)

| Error message | Definition |
|---|---|
| Firmware update is in progress. Try again later. | A user tries to save the CMM configuration to the Lenovo Flex System chassis midplane while the CMM firmware is updating. |
| Incomplete or malformed URL. | The user tries to use an invalid URL. |
| Option argument for -p exceeds max length (31 characters): *passphrase*<br>where *passphrase* is the passphrase that was entered. | A user tries to enter a passphrase that is too long. |
| Passphrase must have at least 6 characters. | A user tries to enter a passphrase that is too short. |
| Please provide a backup file name at the end of the URL | A user tries to enter a backup file name without specifying the file name. |
| Please provide a file name at the end of the URL | The user tries to enter a URL without the required file name. |
| Protocol string length exceeds max of 8 | The user tries to enter a protocol string that is too long. |
| There was a problem downloading the file | The user does not have the authority for downloading or an error occurs when downloading. |
| Upload failed, there was a problem uploading the file | The CMM is unable to upload the file to the user specified server. |
| URL Length exceeds max of 256 | The user tries to enter a URL that is too long. |

# 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://static.lenovo.com/us/en/serverproven/index.shtml 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 http://www.ibm.com/support/entry/portal/Open_service_request 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 service data

You can use the Enhanced Customer Data Repository to send diagnostic data.

Before you send diagnostic data, 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 http://www.ibm.com/planetwide for support telephone numbers. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

## Hardware service and support

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 http://www.ibm.com/partnerworld and click **Business Partner Locator**. For IBM support telephone numbers, see http://www.ibm.com/planetwide. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

In the U.S. and Canada, hardware service and support is available 24 hours a day, 7 days a week. In the U.K., these services are available Monday through Friday, from 9 a.m. to 6 p.m.

## Taiwan product service

Use this information to contact product service for Taiwan.

委製商/進口商名稱: 荷蘭商聯想股份有限公司台灣分公司
進口商地址: 台北市內湖區堤頂大道2段89號5樓
進口商電話: 0800-000-702 (代表號)

# Appendix B. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area.

Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

*Lenovo (United States), Inc.*  
*1009 Think Place - Building One*  
*Morrisville, NC 27560*  
*U.S.A.*  
*Attention: Lenovo Director of Licensing*

LENOVO PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

## Trademarks

Lenovo, the Lenovo logo, Flex System, System x, NeXtScale System, and x Architecture are trademarks of Lenovo in the United States, other countries, or both.

Intel and Intel Xeon are trademarks of Intel Corporation in the United States, other countries, or both.

Internet Explorer, Microsoft, and Windows are trademarks of the Microsoft group of companies.

Linux is a registered trademark of Linus Torvalds.

Other company, product, or service names may be trademarks or service marks of others.

## Important notes

Processor speed indicates the internal clock speed of the microprocessor; other factors also affect application performance.

CD or DVD drive speed is the variable read rate. Actual speeds vary and are often less than the possible maximum.

When referring to processor storage, real and virtual storage, or channel volume, KB stands for 1 024 bytes, MB stands for 1 048 576 bytes, and GB stands for 1 073 741 824 bytes.

When referring to hard disk drive capacity or communications volume, MB stands for 1 000 000 bytes, and GB stands for 1 000 000 000 bytes. Total user-accessible capacity can vary depending on operating environments.

Maximum internal hard disk drive capacities assume the replacement of any standard hard disk drives and population of all hard-disk-drive bays with the largest currently supported drives that are available from Lenovo.

Maximum memory might require replacement of the standard memory with an optional memory module.

Each solid-state memory cell has an intrinsic, finite number of write cycles that the cell can incur. Therefore, a solid-state device has a maximum number of write cycles that it can be subjected to, expressed as `total bytes written` (TBW). A device that has exceeded this limit might fail to respond to system-generated commands or might be incapable of being written to. Lenovo is not responsible for replacement of a device that has exceeded its maximum guaranteed number of program/erase cycles, as documented in the Official Published Specifications for the device.

Lenovo makes no representations or warranties with respect to non-Lenovo products. Support (if any) for the non-Lenovo products is provided by the third party, not Lenovo.

Some software might differ from its retail version (if available) and might not include user manuals or all program functionality.

## Recycling information

Lenovo encourages owners of information technology (IT) equipment to responsibly recycle their equipment when it is no longer needed. Lenovo offers a variety of programs and services to assist equipment owners in recycling their IT products. For information on recycling Lenovo products, go to: http://www.lenovo.com/recycling.

US & Canada Only

US & Canada Only

## Particulate contamination

**Attention:** Airborne particulates (including metal flakes or particles) and reactive gases acting alone or in combination with other environmental factors such as humidity or temperature might pose a risk to the device that is described in this document.

Risks that are posed by the presence of excessive particulate levels or concentrations of harmful gases include damage that might cause the device to malfunction or cease functioning altogether. This specification sets forth limits for particulates and gases that are intended to avoid such damage. The limits must not be viewed or used as definitive limits, because numerous other factors, such as temperature or moisture content of the air, can influence the impact of particulates or environmental corrosives and gaseous contaminant transfer. In the absence of specific limits that are set forth in this document, you must implement practices that maintain particulate and gas levels that are consistent with the protection of human health and safety. If Lenovo determines that the levels of particulates or gases in your environment have caused damage to the device, Lenovo may condition provision of repair or replacement of devices or parts on implementation of appropriate remedial measures to mitigate such environmental contamination. Implementation of such remedial measures is a customer responsibility.

*Table 158. Limits for particulates and gases*

| Contaminant | Limits |
|---|---|
| Particulate | • The room air must be continuously filtered with 40% atmospheric dust spot efficiency (MERV 9) according to ASHRAE Standard 52.2[1].<br>• 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.<br>• The deliquescent relative humidity of the particulate contamination must be more than 60%[2].<br>• The room must be free of conductive contamination such as zinc whiskers. |
| Gaseous | • Copper: Class G1 as per ANSI/ISA 71.04-1985[3]<br>• Silver: Corrosion rate of less than 300 in 30 days |

[1] ASHRAE 52.2-2008 - *Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size*. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

[2] The deliquescent relative humidity of particulate contamination is the relative humidity at which the dust absorbs enough water to become wet and promote ionic conduction.

[3] ANSI/ISA-71.04-1985. *Environmental conditions for process measurement and control systems: Airborne contaminants*. Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.

## Telecommunication regulatory statement

This product may not be certified in your country for connection by any means whatsoever to interfaces of public telecommunications networks. Further certification may be required by law prior to making any such connection. Contact a Lenovo representative or reseller for any questions.

## Electronic emission notices

When you attach a monitor to the equipment, you must use the designated monitor cable and any interference suppression devices that are supplied with the monitor.

## Federal Communications Commission (FCC) statement

**Note:** This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. Lenovo is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that might cause undesired operation.

## Industry Canada Class A emission compliance statement

This Class A digital apparatus complies with Canadian ICES-003.

## Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

## Australia and New Zealand Class A statement

**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

CE

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

## Germany Class A statement

### Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

**Deutschsprachiger EU Hinweis:Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit** Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2014/30/EU (früher 2004/108/EC) zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der Klasse A der Norm gemäß Richtlinie.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der Lenovo empfohlene Kabel angeschlossen werden. Lenovo übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der Lenovo verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der Lenovo gesteckt/eingebaut werden.

**Deutschland:**

**Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Betriebsmittein** Dieses Produkt entspricht dem „Gesetz über die elektromagnetische Verträglichkeit von Betriebsmitteln“ EMVG (früher „Gesetz über die elektromagnetische Verträglichkeit von Geräten“). Dies ist die Umsetzung der EU-Richtlinie 2014/30/EU (früher 2004/108/EC) in der Bundesrepublik Deutschland.

**Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Betriebsmitteln, EMVG vom 20. Juli 2007 (früher Gesetz über die elektromagnetische Verträglichkeit von Geräten), bzw. der EMV EU Richtlinie 2014/30/EU (früher 2004/108/EC), für Geräte der Klasse A.**

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen. Verantwortlich für die Konformitätserklärung nach Paragraf 5 des EMVG ist die Lenovo (Deutschland) GmbH, Meitnerstr. 9, D-70563 Stuttgart.

Informationen in Hinsicht EMVG Paragraf 4 Abs. (1) 4:**Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.**

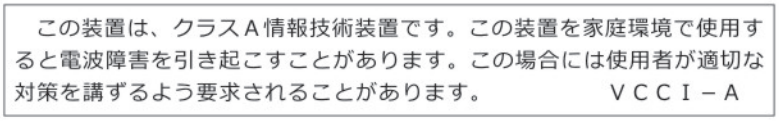
Nach der EN 55022: „Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen und dafür aufzukommen.“

Nach dem EMVG: „Geräte dürfen an Orten, für die sie nicht ausreichend entstört sind, nur mit besonderer Genehmigung des Bundesministers für Post und Telekommunikation oder des Bundesamtes für Post und Telekommunikation betrieben werden. Die Genehmigung wird erteilt, wenn keine elektromagnetischen Störungen zu erwarten sind.“ (Auszug aus dem EMVG, Paragraph 3, Abs. 4). Dieses Genehmigungsverfahren ist nach Paragraph 9 EMVG in Verbindung mit der entsprechenden Kostenverordnung (Amtsblatt 14/93) kostenpflichtig.

Anmerkung: Um die Einhaltung des EMVG sicherzustellen sind die Geräte, wie in den Handbüchern angegeben, zu installieren und zu betreiben.

## Japanese electromagnetic compatibility statements

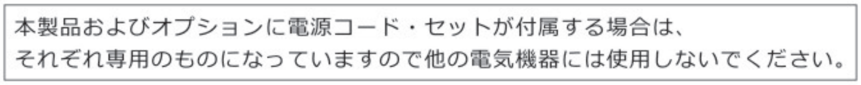
### Japan VCCI Class A statement



この装置は、クラスＡ情報技術装置です。この装置を家庭環境で使用すると電波障害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。　ＶＣＣＩ－Ａ

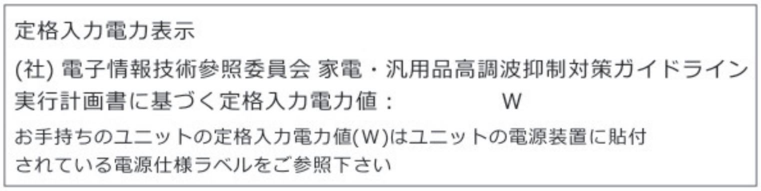
This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI). If this equipment is used in a domestic environment, radio interference may occur, in which case the user may be required to take corrective actions.

### Japanese Electrical Appliance and Material Safety Law statement (for detachable AC power cord)



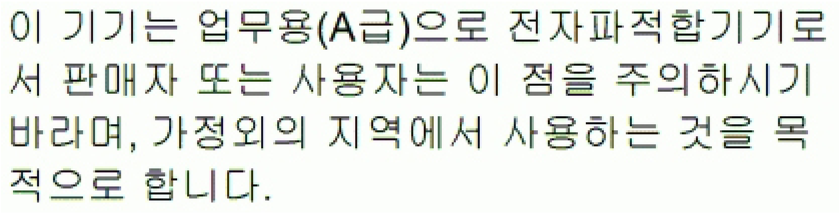
本製品およびオプションに電源コード・セットが付属する場合は、
それぞれ専用のものになっていますので他の電気機器には使用しないでください。

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



定格入力電力表示
(社) 電子情報技術参照委員会 家電・汎用品高調波抑制対策ガイドライン
実行計画書に基づく定格入力電力値：　W
お手持ちのユニットの定格入力電力値(W)はユニットの電源装置に貼付
されている電源仕様ラベルをご参照下さい

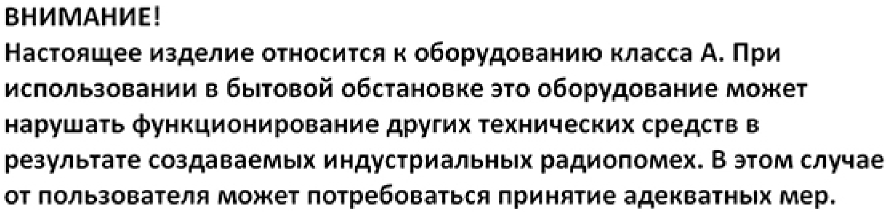
## Korea Communications Commission (KCC) statement



이 기기는 업무용(A급)으로 전자파적합기기로
서 판매자 또는 사용자는 이 점을 주의하시기
바라며, 가정외의 지역에서 사용하는 것을 목
적으로 합니다.

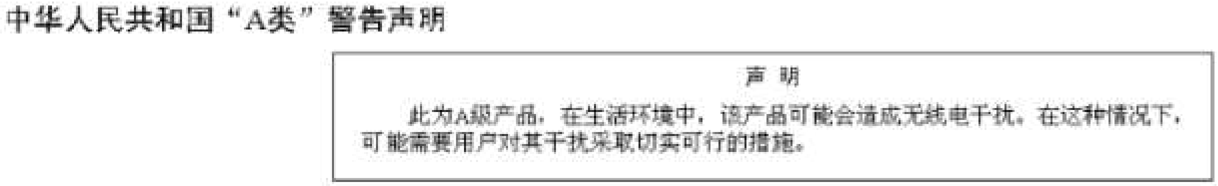
This is electromagnetic wave compatibility equipment for business (Type A). Sellers and users need to pay attention to it. This is for any areas other than home.

## Russia Electromagnetic Interference (EMI) Class A statement



ВНИМАНИЕ!
Настоящее изделие относится к оборудованию класса А. При
использовании в бытовой обстановке это оборудование может
нарушать функционирование других технических средств в
результате создаваемых индустриальных радиопомех. В этом случае
от пользователя может потребоваться принятие адекватных мер.

## People's Republic of China Class A electronic emission statement

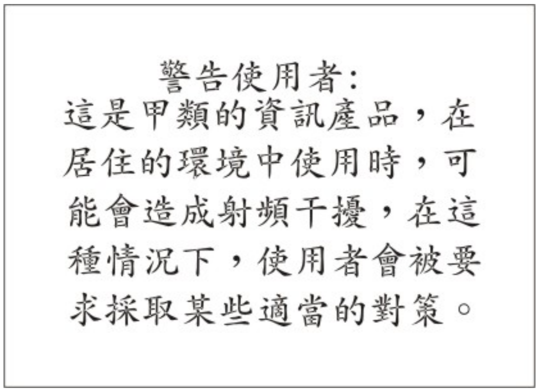


中华人民共和国“A类”警告声明

声明

此为A级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

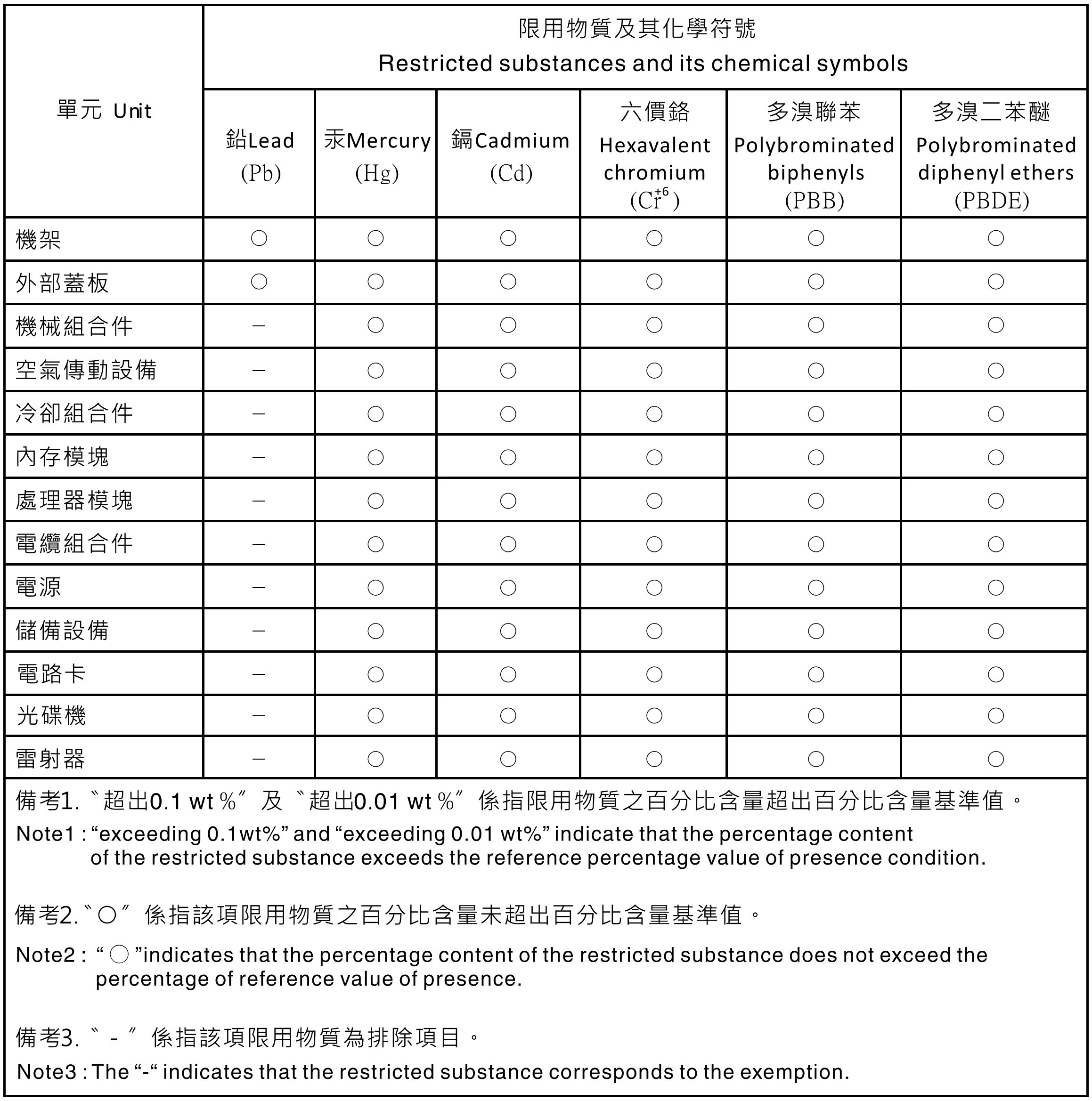
## Taiwan Class A compliance statement



警告使用者:

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

## Taiwan BSMI RoHS declaration



| 單元 Unit | 限用物質及其化學符號<br>Restricted substances and its chemical symbols | | | | | |
|---|---|---|---|---|---|---|
| | 鉛Lead<br>(Pb) | 汞Mercury<br>(Hg) | 鎘Cadmium<br>(Cd) | 六價鉻<br>Hexavalent chromium<br>($Cr^{+6}$) | 多溴聯苯<br>Polybrominated biphenyls<br>(PBB) | 多溴二苯醚<br>Polybrominated diphenyl ethers<br>(PBDE) |
| 機架 | ○ | ○ | ○ | ○ | ○ | ○ |
| 外部蓋板 | ○ | ○ | ○ | ○ | ○ | ○ |
| 機械組合件 | – | ○ | ○ | ○ | ○ | ○ |
| 空氣傳動設備 | – | ○ | ○ | ○ | ○ | ○ |
| 冷卻組合件 | – | ○ | ○ | ○ | ○ | ○ |
| 內存模塊 | – | ○ | ○ | ○ | ○ | ○ |
| 處理器模塊 | – | ○ | ○ | ○ | ○ | ○ |
| 電纜組合件 | – | ○ | ○ | ○ | ○ | ○ |
| 電源 | – | ○ | ○ | ○ | ○ | ○ |
| 儲備設備 | – | ○ | ○ | ○ | ○ | ○ |
| 電路卡 | – | ○ | ○ | ○ | ○ | ○ |
| 光碟機 | – | ○ | ○ | ○ | ○ | ○ |
| 雷射器 | – | ○ | ○ | ○ | ○ | ○ |

備考1. 〝超出0.1 wt %〞 及 〝超出0.01 wt %〞 係指限用物質之百分比含量超出百分比含量基準值。

Note1 : “exceeding 0.1wt%” and “exceeding 0.01 wt%” indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.

備考2. 〝○〞 係指該項限用物質之百分比含量未超出百分比含量基準值。

Note2 : “ ○ ”indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.

備考3. 〝 - 〞 係指該項限用物質為排除項目。

Note3 : The “-“ indicates that the restricted substance corresponds to the exemption.

# Index

Part Number: SP47A31782

Printed in China

(1P) P/N: SP47A31782