



# Flex System Chassis Management Module Command-Line Interface Reference Guide (For Type 7893, 8721, and 8724 chassis only)



## Note

Before using this information and the product it supports, read the general information in Appendix B “Notices” on page 465, the *Warranty Information* document, and the *Safety Information* and the *Environmental Notices and User Guide* documents on the Lenovo documentation CD.

Sixth Edition (April 2018)

© Copyright Lenovo 2015, 2018.

**LIMITED AND RESTRICTED RIGHTS NOTICE:** If data or software is delivered pursuant to a General Services Administration “GSA” contract, use, reproduction, or disclosure is subject to restrictions set forth in Contract No. GS-35F-05925

---

# Contents

## Chapter 1. Introduction . . . . . 1

Before you begin . . . . .	1
Notices and statements in this document . . . . .	2
Accessibility features for the Flex SystemCMM . . . . .	2

## Chapter 2. Command-line interface use and reference . . . . . 5

Command-line interface guidelines . . . . .	5
Command targets . . . . .	6
Commands and user authority . . . . .	10
Cabling the CMM . . . . .	14
Networked connection . . . . .	15
Direct client connection . . . . .	15
Serial cable connection . . . . .	16
Starting the command-line interface . . . . .	16
CMM network access tag . . . . .	17
IPv6 addressing for initial connection . . . . .	18
Telnet connection . . . . .	19
Serial connection . . . . .	20
Secure Shell (SSH) connection . . . . .	21
Configuring Flex System Enterprise Chassis components by using the CLI . . . . .	23
Configuring the CMM for CLI operation . . . . .	24
Serial over LAN . . . . .	26
Starting an SOL session . . . . .	26
Ending an SOL session . . . . .	27
Specifying a URL for file transfer . . . . .	27
External authentication of certificates . . . . .	28
Importing an LDAP certificate with non-mutual authentication . . . . .	30
Importing an LDAP certificate with mutual authentication . . . . .	31

## Chapter 3. Command reference . . . . . 35

accsecfg command . . . . .	35
advfailover command . . . . .	45
airfilter command . . . . .	47
alertcfg command . . . . .	48
alertentries command . . . . .	50
autoftp command . . . . .	57
baydata command . . . . .	59
bootmode command . . . . .	64
bootseq command . . . . .	66
chconfig command . . . . .	69
chlog command . . . . .	76
chmanual command . . . . .	79
cimsub command . . . . .	81

cin command . . . . .	84
cinstatus command . . . . .	90
clear command . . . . .	91
clearlog command . . . . .	93
config command . . . . .	95
console command . . . . .	100
coolingzones command . . . . .	101
crypto command . . . . .	103
date command . . . . .	106
dhcpcfg command . . . . .	108
displaylog command . . . . .	112
displaysd command . . . . .	118
dns command . . . . .	120
env command . . . . .	124
ethoverusb command . . . . .	129
events command . . . . .	131
exit command . . . . .	133
files command . . . . .	134
fod command . . . . .	135
fruactlog command . . . . .	136
fsmcm command . . . . .	137
fuelg command . . . . .	139
groups command . . . . .	150
health command . . . . .	156
help command . . . . .	160
history command . . . . .	163
ifconfig command . . . . .	164
info command . . . . .	192
iocomp command . . . . .	199
ldapcfg command . . . . .	201
led command . . . . .	211
list command . . . . .	214
monalerts command . . . . .	215
ntp command . . . . .	224
permggroups command . . . . .	228
ping command . . . . .	232
pmpolicy command . . . . .	235
portcfg command . . . . .	237
ports command . . . . .	240
power command . . . . .	254
pwrprofile command . . . . .	260
read command . . . . .	269
remotechassis command . . . . .	273
reset command . . . . .	277
scale command . . . . .	279
sddump command . . . . .	284

sdemail command . . . . .	286	events command errors. . . . .	409
security command . . . . .	287	exit command errors . . . . .	409
service command . . . . .	290	files command errors. . . . .	410
smtp command . . . . .	293	fod command errors . . . . .	410
snmp command . . . . .	295	fruactlog command errors. . . . .	411
sol command. . . . .	308	fsmcm command errors . . . . .	411
sshcfg command . . . . .	315	fuelg command errors . . . . .	411
sslcfg command . . . . .	317	groups command errors . . . . .	415
syslog command . . . . .	328	health command errors . . . . .	416
tcpcmdmode command . . . . .	333	help command errors . . . . .	417
temps command . . . . .	336	history command errors . . . . .	417
trespass command . . . . .	337	ifconfig command errors . . . . .	417
uicfg command . . . . .	339	info command errors . . . . .	421
update command . . . . .	343	iocomp command errors . . . . .	422
uplink command . . . . .	349	ldapcfg command errors . . . . .	422
users command. . . . .	353	led command errors . . . . .	423
vlan command . . . . .	371	list command errors . . . . .	424
volts command . . . . .	382	monalerts command errors . . . . .	424
write command . . . . .	383	ntp command errors . . . . .	424
<b>Chapter 4. Error messages . . . . .</b>	<b>385</b>	permggroups command errors . . . . .	425
Common errors . . . . .	385	ping command errors . . . . .	426
accseccfg command errors . . . . .	387	pmpolicy command errors . . . . .	427
advfailover command errors . . . . .	389	portcfg command errors . . . . .	427
airfilter command errors . . . . .	389	ports command errors . . . . .	427
alertcfg command errors . . . . .	389	power command errors. . . . .	429
alertentries command errors . . . . .	389	pwrprofile command errors . . . . .	431
autoftp command errors . . . . .	390	read command errors . . . . .	433
baydata command errors . . . . .	391	remotechassis command errors . . . . .	434
bootmode command errors . . . . .	392	reset command errors . . . . .	435
bootseq command errors . . . . .	392	scale command errors . . . . .	437
chconfig command errors . . . . .	393	sddump command errors . . . . .	437
chlog command errors . . . . .	395	sdemail command errors . . . . .	438
chmanual command errors . . . . .	396	security command errors . . . . .	438
cimsub command errors . . . . .	396	service command errors . . . . .	438
cin command errors . . . . .	397	smtp command errors . . . . .	439
cinstatus command errors . . . . .	398	snmp command errors . . . . .	440
clear command errors . . . . .	398	sol command errors . . . . .	440
clearlog command errors . . . . .	399	sshcfg command errors . . . . .	442
config command errors . . . . .	399	sslcfg command errors . . . . .	442
console command errors . . . . .	400	syslog command errors. . . . .	444
coolingzones command errors . . . . .	401	tcpcmdmode command errors . . . . .	445
crypto command errors. . . . .	402	temps command errors. . . . .	446
date command errors . . . . .	403	trespass command errors . . . . .	446
dhcpinfo command errors. . . . .	404	uicfg command errors . . . . .	446
displaylog command errors . . . . .	404	update command errors . . . . .	447
displaysd command errors . . . . .	406	uplink command errors . . . . .	451
dns command errors . . . . .	408	users command errors . . . . .	452
env command errors . . . . .	408	vlan command errors. . . . .	456
ethoverusb command errors. . . . .	408	volts command errors . . . . .	459
		write command errors . . . . .	459

---

**Appendix A. Getting help and technical assistance . . . . .461**

Before you call . . . . . 461  
Using the documentation . . . . . 462  
Getting help and information from the World Wide Web . . . . . 462  
How to send DSA data . . . . . 462  
Creating a personalized support web page . . . . 462  
Software service and support . . . . . 463  
Hardware service and support . . . . . 463  
Taiwan product service . . . . . 463

**Appendix B. Notices. . . . .465**

Trademarks . . . . . 466  
Important notes . . . . . 466  
Recycling information . . . . . 466  
Particulate contamination . . . . . 467  
Telecommunication regulatory statement. . . . . 467  
Electronic emission notices . . . . . 467

Federal Communications Commission (FCC) statement . . . . . 468  
Industry Canada Class A emission compliance statement . . . . . 468  
Avis de conformité à la réglementation d'Industrie Canada. . . . . 468  
Australia and New Zealand Class A statement . . . . . 468  
European Union EMC Directive conformance statement . . . . . 468  
Germany Class A statement . . . . . 468  
Japan VCCI Class A statement . . . . . 469  
Korea Communications Commission (KCC) statement . . . . . 470  
Russia Electromagnetic Interference (EMI) Class A statement . . . . . 470  
People's Republic of China Class A electronic emission statement . . . . . 470  
Taiwan Class A compliance statement . . . . . 470

**Index . . . . .471**



---

## Chapter 1. Introduction

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

**Note:** The Flex System Chassis Management Module is compatible with only Type 7893, 8721, and 8724 chassis.

Using the CLI, you can issue commands to control the power and configuration of the CMM and other components that are in an Flex System Enterprise 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.

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 the Flex System Enterprise 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 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 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 100 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 Flex System components. Go to <http://>

[datacentersupport.lenovo.com](http://datacentersupport.lenovo.com) for the latest information about upgrading the device drivers, firmware, and UEFI code for 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 Flex SystemCMM

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 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 Flex System by using the optional Flex System Manager management software, see the Flex System Manager documentation for information about its accessibility features.

The 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 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 Flex System information center.



**Lenovo and accessibility**

See Human Ability and Accessibility Center 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 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 14
- “Starting the command-line interface” on page 16
- “Configuring Flex System Enterprise Chassis components by using the CLI” on page 23
- “Configuring the CMM for CLI operation” on page 24
- “Serial over LAN” on page 26
- “Specifying a URL for file transfer” on page 27
- “External authentication of certificates” on page 28

See Chapter 3 “Command reference” on page 35 for detailed information about commands that are used to monitor and control Flex System components. Command-line interface error messages are in Chapter 4 “Error messages” on page 385. 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 Enterprise 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 Enterprise 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 and IBM 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 Enterprise Chassis, use the “list command” on page 214.

Table 1. Valid command targets

Component	Target path
Flex System Enterprise Chassis	<code>system</code>
CMM (by bay number)	<code>mm[x]</code>
CMM (primary)	<code>mm[p]</code> or <code>mm[P]</code>
CMM (standby)	<code>mm[s]</code> or <code>mm[S]</code>
Compute node	<code>blade[x]</code>
Logical node grouping	<code>bladegroup[x]</code>

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)	flashdim[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 124). 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 **-Tsystem:mm[1]** option to redirect a command to the CMM in bay 1.
- Use the **-Tsystem:switch[1]** option to redirect a command to the I/O module in I/O bay 1.
- Use the **-Tsp** 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 **-Tblade[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 Enterprise Chassis.

Most CMM commands must be directed to the primary CMM. If only one CMM is installed in the Flex System Enterprise 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 214).

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 Enterprise Chassis, while the Flex System Enterprise 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 Enterprise Chassis.

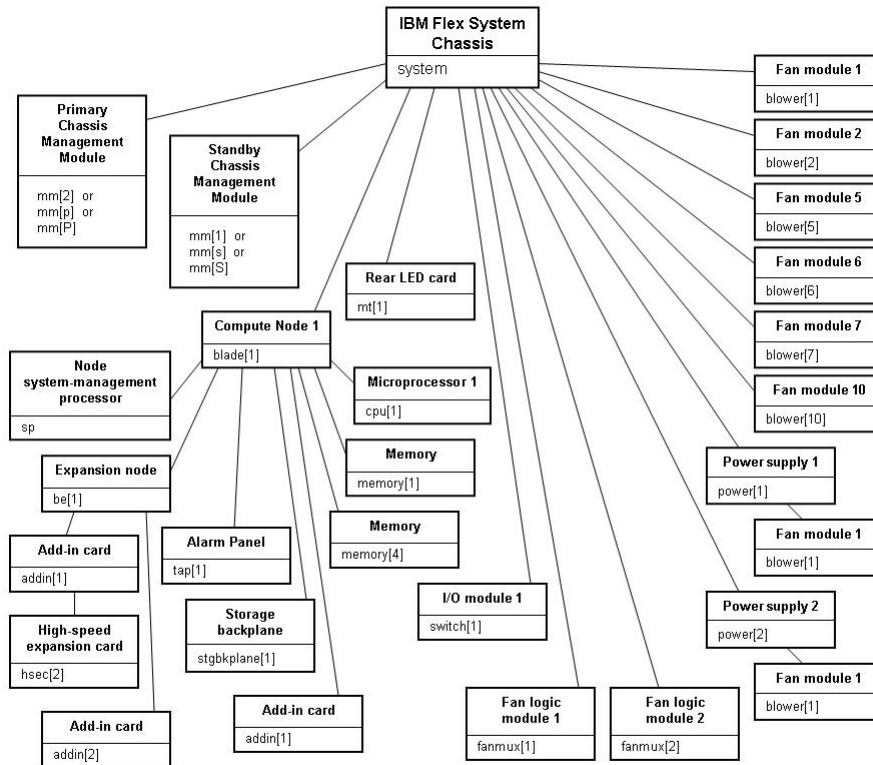
Table 2. Example system components and command paths

Component	Target path
Flex System Enterprise Chassis	system
Compute node, bay 1 (named 'Server1')	system:blade[1]
Node system-management processor, compute node bay 1	system:blade[1]:sp

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

Component	Target path
Microprocessor, compute node bay 1	system:blade[1]:cpu[1]
Alarm panel, compute node bay 1	system:blade[1]:tap[1]
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 Enterprise 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 2 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 diamond (◊). 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 Enterprise Chassis are controlled by the CMM in each Flex System Enterprise Chassis, using the CMM CLI “users command” on page 353 and the “permggroups command” on page 228 or the CMM web interface. If your Flex System configuration includes an optional Flex System Manager management node, users and permission groups for each optional Flex System Manager installation are controlled by the optional Flex System Manager management software (see [http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.8731.doc/product\\_page.html](http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.8731.doc/product_page.html) for information).

**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 201 for information.

Table 3. Command authority relationships

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
accseccfg	•				•					
advfailover	•				•					
airfilter	•	•	•	•	•					
alertcfg	•				•					
alertentries	•	•	•	•	•					
baydata	•						•			
bootmode	•						•			
chconfig	•				•					
chlog	•				•					
chmanual	•	•	•	•	•	•	•	•	•	•
cimsub	•									
cin	•	◊			◊					
clear	•			◊	◊				◊	◊
clearlog	•		•							

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
config (compute node target)	.						.			
config (CMM or Flex System Enterprise Chassis)	.				.					
console	.							.		
crypto	.				.					
date	.				.					
dns	.				.					
events -che	.	.	.	.	.	.	.	.	.	.
events -che -add -rm	.				.					
files -d	.			.	.	.	.		.	.
fsmcm	.	.								
fuelg	.				.					
groups	.				.					
ifconfig (compute node target)	.						.			
ifconfig (compute node ISMP, CMM, and system targets)	.				.					
ifconfig (I/O module target)	.									.
ifconfig -pip (I/O module target)	.								.	.
ldapcfg	.				.					
led -info, -loc (system target)	.			.						
led -info, -loc (compute node target)	.					.				
led -loc (I/O module target)	.								.	
monalerts	.				.					
ntp	.				.					
permggroups	.	.								

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
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 <sup>1</sup>	.				.					
reset (compute node or ISMP target)	.					.				
reset (I/O module target)	.								.	
reset (CMM target)	.			.						
reset -c, -sft, (compute node target)	.					◇		◇		
reset -exd, -full, -std (I/O module target)	.								.	
reset -f, -standby (CMM target)	.			.						
sddump	.					.				
sdemail	.	.	.	.	.	.	.	.	.	.
security	.				.					
service (CMM target)	.			.	.					
service (compute node or storage 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
service (compute node system-management processor target)	.						.			
service (I/O module target)	.								.	
smtp	.				.					
snmp	.				.					
sol	.				.		.			
sshcfg	.				.					
sslcfg	.				.					
syslog	.	.	.	.	.					
tcpcmdmode	.				.					
trespass	.				.					
uicfg	.				.					
update (CMM target)	.			.						
update (I/O module target)	.								.	
uplink	.				.					
users	.	.								
vlan (CMM target)	.				.					
vlan (chassis 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 the Flex System Enterprise Chassis. The CMM supports Ethernet (local or remote) and serial management connections.

You can manage the Flex System Enterprise Chassis by using the 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 Enterprise 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 the Flex System Enterprise 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 the *Flex System Chassis Management Module 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 *Flex System Chassis Management Module 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 *Flex System Chassis Management Module 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 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 Flex System 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 Enterprise 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 18 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: PASSWORD (note the number zero, not the letter O, in PASSWORD)

For IPv4, the system that you are connecting to the CMM must be configured to operate on the same subnet as the Flex SystemCMM. 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 Enterprise 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 an Flex System Enterprise Chassis.

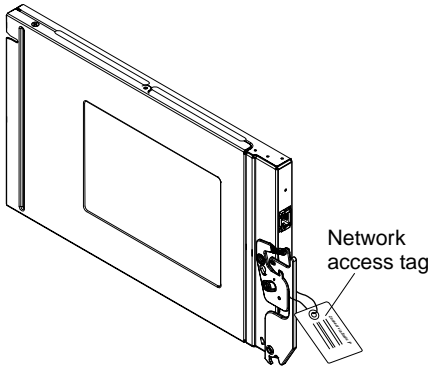
The network access tag lists the following initial connection information for the CMM:

- 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 (PASSWORD, note the number zero, not the letter O, in PASSWORD)

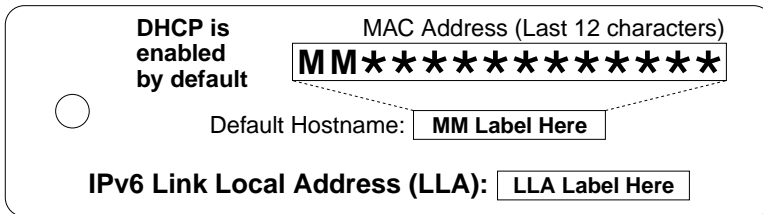
The network access tag is attached to the front of the CMM, as shown in the following illustration.

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



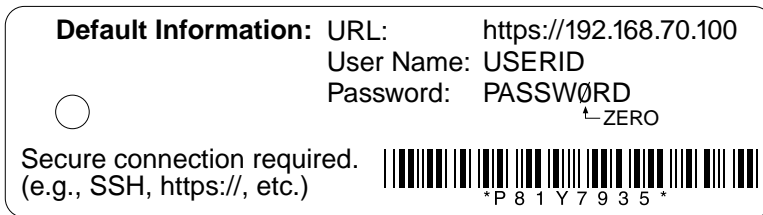
The front of the network access tag lists the CMM MAC address, default host name, and IPv6 link local address (LLA), as shown in the following illustration.

### Front



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

### Rear



## IPv6 addressing for initial connection

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

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

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



- Read the CMM link-local address on the network access tag that is attached to the front of the CMM (see “CMM network access tag” on page 17 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 164 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 MMxxxxxxxxxx, 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:

- 001110**01**-A7-94-FF-FE-07-CB-D0
- 001110**11**-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:CB D0

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

**FE80::3BA7:94FF:FE07:CB D0**

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:CB D0.

## 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 MMxxxxxxxxxxx, 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 *Flex System Chassis Management Module Installation Guide*, for the location of the reset button). See "IPv6 addressing for initial connection" on page 18 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 PASSWORD (note the number zero, not the letter O, in PASSWORD).

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 Enterprise Chassis (see "Configuring the CMM," in the *Flex System Chassis Management Module 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 *Flex System Chassis Management Module 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 277 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 PASSWORD (note the number zero, not the letter O, in PASSWORD).

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 Enterprise Chassis (see “Configuring the CMM,” in the *Flex System Chassis Management Module 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 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 240 for information about command use).
  - Enable the SSH server by using the **sshcfg -cstatus** command (see “sshcfg command” on page 315 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 MMxxxxxxxxxxx, 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 18 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 PASSWORD (note the number zero, not the letter O, in PASSWORD).

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 Enterprise Chassis (see "Configuring the CMM," in the *Flex System Chassis Management Module 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 315.

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.
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.

## Configuring Flex System Enterprise Chassis components by using the CLI

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

The Flex System Enterprise Chassis automatically detects the modules and compute nodes that are installed and stores the vital product data (VPD). When the Flex System Enterprise Chassis is started, the CMM automatically configures the remote management and console (Ethernet) connector of the CMM, so that you can configure and manage Flex System components. You configure and manage 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 *Flex System Chassis Management Module User's Guide* for information). The optional Flex System Manager software also supports selected configuration and management functions for the Flex System Enterprise Chassis.

To manually configure the basic settings for an Flex System Enterprise 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 24 for information).
- Step 2. Start a CMM CLI session (see "Starting the command-line interface" on page 16 for information).
- Step 3. View the installed components in the Flex System Enterprise Chassis and their health status by using the list command (see "list command" on page 214 for information) and health command (see "health command" on page 156 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 95 for information).
- Step 5. Set the system date and time by using the `date` command (see “date command” on page 106 for information).
- Step 6. Verify the CMM IP configuration by using the `ifconfig` command (see “ifconfig command” on page 164 for information).
- Step 7. Set up credentials of the main supervisor user account (USERID) by using the `users` command (see “users command” on page 353 for information).
- Step 8. To communicate with network resources and with components in the Flex System Enterprise 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 Flex System Enterprise 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 240 for information).
    - b. Configure IP addresses for the I/O modules by using the `ifconfig` command (see “ifconfig command” on page 164 for information).
- Step 9. Set the overall CMM security policy by using the `security` command (see “security command” on page 287 for information).
  - Step 10. Set the CMM DNS configuration by using the `dns` command (see “dns command” on page 120 for information).
  - Step 11. Set an email address for CMM event notifications by using the `alertentries` command (see “alertentries command” on page 50 for information).

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

If the CMM that you are installing is the only CMM in the Flex System Enterprise 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 269 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 164 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 Flex System Enterprise 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 108 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 16 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 164 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 164 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 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 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 26). 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 *Flex System Chassis Management Module 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 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 Flex System Enterprise Chassis and the compute node before you can start an SOL session with the compute node. See “sol command” on page 308 for information about setting up and enabling SOL.

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

Start an SOL session by using the **console** command (see “console command” on page 100 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 308 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

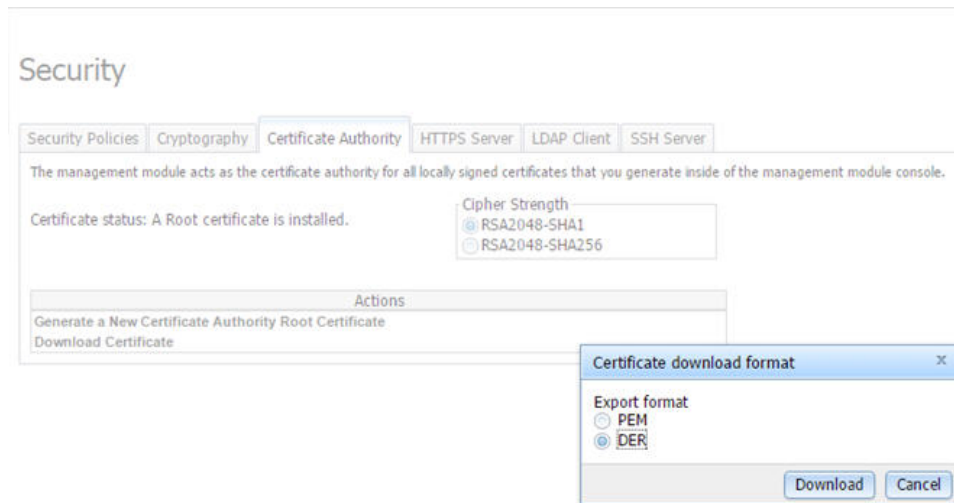
Certificates are used to establish secure, trusted connections to the CMM and from the CMM to other servers.

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 the Flex System Enterprise Chassis. 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 Flex System Enterprise 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 > Certificate Authority > Download Certificate**. Select the certificate format, and click **Download**.
- In the CLI, download the CA certificate into the CMM by using the `sslcfg -dnld` command (see “`sslcfg` command” on page 317 for additional information about command use).

The following illustration shows the "Certificate download format" window.



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 Enterprise 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 Flex System Enterprise 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 IBM 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, into the Certificate Trust Store of your Flex System Manager management software, into any 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 31 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 Flex System Enterprise 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 16 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 124 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 317 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 27.

## 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 30.
2. Start a CMM CLI session (see “Starting the command-line interface” on page 16 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 124 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 317 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 317 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 27.

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 16 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 124 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 317 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 317 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 317 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 27.

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 317 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 27.

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 Flex System Enterprise 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 31, or, if the chassis policy allows, export a CSR from each management component, get it signed, and import it back into the corresponding Flex System Enterprise Chassis management component.





---

## Chapter 3. Command reference

Each command topic describes an Flex SystemChassis Management Module 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.

---

### accsecfg 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 385 for a list of error messages that apply to all commands or “accsecfg command errors” on page 387 for a list of error messages that are specific to the accsecfg command.

Table 5. *accseccfg* command

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

Table 5. `accseccfg` command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
	<ul style="list-style-type: none"> <li>• -dc (minimum number of different password characters): 0</li> <li>• -de (default account password change at next login): off</li> <li>• -ia (account inactivity alert time period): 0</li> <li>• -ici (log new login events from same user): retains set value</li> <li>• -id (account inactivity disable time): 0</li> <li>• -lf (maximum login failures): 20</li> <li>• -lp (lockout period after maximum login failures): 2</li> <li>• -mls (maximum simultaneous user sessions): retains set value</li> <li>• -pc (password change on first access): off</li> <li>• -pe (password expiration time): 0</li> <li>• -pi (minimum password change interval): 0</li> <li>• -rc (password reuse cycle): 0</li> <li>• -wt (web inactivity session timeout): retains set value</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• Modifying any default values after setting the -legacy or -secure option changes the user account security setting indication to custom.</li> <li>• Accounts can not be set to -legacy if the CMM chassis security level is set to secure by the “security command” on page 287.</li> <li>• The user who is running the <code>accseccfg -legacy</code> command must have a password assigned.</li> <li>• The -legacy option must be run alone and not in conjunction with any other <code>accseccfg</code> command options.</li> </ul>		
<p><b>Set account security defaults to high level</b></p>	<p>Sets CMM account security to a predefined high set of default values. High default values are:</p> <ul style="list-style-type: none"> <li>• -alt (authentication logging timeout): retains set value</li> <li>• -am (user authentication method): retains set value</li> <li>• -cp (complex password): on</li> <li>• -ct (CLI inactivity session timeout): retains set value</li> <li>• -dc (minimum number of different password characters): 2</li> </ul>	<p><code>accseccfg -high</code></p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>

Table 5. *accseccfg* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
	<ul style="list-style-type: none"> <li>• -de (default account password change at next login): on</li> <li>• -ia (account inactivity alert time period): 120</li> <li>• -ici (log new login events from same user): retains set value</li> <li>• -id (account inactivity disable time): 180</li> <li>• -lf (maximum login failures): 20</li> <li>• -lp (lockout period after maximum login failures): 60</li> <li>• -pc (password change on first access): on</li> <li>• -pe (password expiration time): 90</li> <li>• -pi (minimum password change interval): 24</li> <li>• -rc (password reuse cycle): 5</li> <li>• -wt (web inactivity session timeout): retains set value</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• Modifying any default values after setting the -legacy or -secure option changes the user account security setting indication to custom.</li> <li>• The user who is running the accseccfg -high command must have a password assigned.</li> <li>• The -high option must be run alone and not in conjunction with any other accseccfg command options.</li> </ul>		
<p><b>Set authentication logging timeout</b></p>	<p>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.</p> <p><b>Note:</b> When managing the Flex System Enterprise Chassis with a program that uses the Common Information Model (CIM) interface, such as the optional Flex System Manager program, 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.</p>	<p>accseccfg -alt <i>timeout</i> where <i>timeout</i> 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.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>

Table 5. *accseccfg* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Set user authentication method</b>	<p>Sets a custom value for CMM user authentication method.</p> <p><b>Important:</b> If the authentication method is set to <i>ldap</i> (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.</p>	<p><i>accseccfg -am method</i> where <i>method</i> is</p> <ul style="list-style-type: none"> <li>• local</li> <li>• ldap</li> <li>• localldap</li> <li>• ldaplocal</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>
<b>Enable / disable complex password</b>	<p>Enables or disables the complex password for CMM user authentication.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• -cp must be on to set the CMM chassis security level to secure with the “security command” on page 287.</li> <li>• -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.</li> <li>• The user that is running the <i>accseccfg -cp</i> command must have a password assigned.</li> </ul>	<p><i>accseccfg -cp state</i> where <i>state</i> is on or off .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>
<b>Set CLI inactivity timeout</b>	<p>Sets the custom value for CMM CLI inactivity session timeout.</p>	<p><i>accseccfg -ct timeout</i> where <i>timeout</i> is from 0 to 4,294,967,295 seconds, inclusive.</p> <p>This command can only be run by users who have the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>

Table 5. *accseccfg* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Set minimum number of different characters for password</b></p>	<p>Sets custom value for the minimum number of different characters to be used in a CMM password.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• The minimum number of different characters applies only when complex passwords are enabled (-cp on). Setting -cp to off will set -dc to 0.</li> <li>• 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.</li> <li>• 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.</li> </ul>	<p><i>accseccfg -dc number</i> where <i>number</i> is from 0 to 15, inclusive.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>
<p><b>Enable / disable default administration password expiration</b></p>	<p>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.</p> <p><b>Note:</b> -de must be on to set the CMM chassis security level to secure with the “security command” on page 287.</p>	<p><i>accseccfg -de state</i> where <i>state</i> is on or off .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>
<p><b>Set account inactivity alert time</b></p>	<p>Sets custom value for CMM account inactivity alert time.</p> <p><b>Note:</b> The <i>accseccfg -ia</i> value must be less than the <i>accseccfg -id</i> value.</p>	<p><i>accseccfg -ia time</i> where <i>time</i> is from 0 to 365 days, inclusive.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>

Table 5. *accseccfg* command (continued)

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

Table 5. *accseccfg* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Set lockout period</b>	Sets the custom value for CMM account lockout period, used when the maximum number of login failures is exceeded.	<p><i>accseccfg -lp time</i>            where <i>time</i> is from 0 to 2880 minutes, inclusive.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>
<b>Set maximum LDAP sessions for user</b>	Sets the custom value for the maximum number of simultaneous login sessions allowed for a single LDAP user	<p><i>accseccfg -mls max_sessions</i>            where <i>max_sessions</i> is from 0 to 20, inclusive.</p> <p>This command can only be run by users who have the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>
<b>Enable / disable password change at first login</b>	<p>Enables or disables the mandatory password change at first CMM login.</p> <p>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.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• <i>accseccfg -pc</i> is set to on automatically when <i>accseccfg</i> is set to -high</li> <li>• <i>accseccfg -pc</i> must be on to set the CMM chassis security level to secure with the “security command” on page 287.</li> </ul>	<p><i>accseccfg -pc state</i>            where <i>state</i> is on or off .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>



Table 5. `accseccfg` command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Set password expiration time</b>	Sets custom value for the CMM password expiration time.	<p><code>accseccfg -pe time</code> where <i>time</i> is from 0 to 365 days, inclusive.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where <i>x</i> is the primary CMM bay number.</p>
<b>Set password minimum change interval</b>	<p>Sets custom value for the minimum amount of time between CMM password changes.</p> <p><b>Note:</b> If the minimum password change interval is greater than 0, it must be less than password expiration period.</p>	<p><code>accseccfg -pi time</code> where <i>time</i> is from 0 to 1440 hours, inclusive, and less than password expiration period when that period is greater than 0.</p> <p>This command can only be run by users who have the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where <i>x</i> is the primary CMM bay number.</p>

Table 5. *accseccfg* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Set password reuse cycle</b>	<p>Sets custom value for the CMM password reuse cycle. This setting determines how many times a password must be changed before being reused.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>-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.</li> <li>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.</li> </ul>	<p><i>accseccfg -rc number_reuses</i> where <i>number_reuses</i> is from 0 to 5, inclusive.</p> <p>This command can only be run by users who have the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>
<b>Set web interface inactivity timeout</b>	<p>Sets custom value for CMM web interface inactivity session timeout.</p>	<p><i>accseccfg -wt timeout</i> where <i>timeout</i> 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).</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>

**Example:**

To set CMM account security to use the legacy level defaults, while the Flex System Enterprise 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 Flex System Enterprise 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 Flex System Enterprise 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.

**Note:** If an Flex System Enterprise 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 Flex System Enterprise Chassis; make sure that the chassis is operating properly before replacing either CMM. See [Troubleshooting chassis](#) for information about diagnosing problems with a Flex System Enterprise 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 385 for a list of error messages that apply to all commands or “advfailover command errors” on page 389 for a list of error messages that are specific to the advfailover command.

Table 6. *advfailover* command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display CMM advanced failover settings</b>	<p>Displays the advanced failover settings for the CMM. Possible return values are:</p> <ul style="list-style-type: none"> <li>off - disable network interface for the standby CMM</li> <li>swap - enable the standby CMM network interface and swap IP addresses between the two CMMs during failover</li> <li>noswap - enable the standby CMM network interface and do not swap IP addresses between the two CMMs during failover</li> </ul> <p><b>Note:</b> When advanced failover is set to off, a CMM failover can be forced using the <code>reset -f</code> command (see “reset command” on page 277 for information).</p>	<code>advfailover</code>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>                      where x is the primary CMM bay number.</p>
<b>Disable network interface for standby CMM</b>	<p>Disables the network interface for the standby CMM, preventing failover.</p> <p><b>Note:</b> When advanced failover is set to off, a CMM failover can be forced using the <code>reset -f</code> command (see “reset command” on page 277 for information).</p>	<p><code>advfailover -ip off</code></p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>                      where x is the primary CMM bay number.</p>
<b>Enable network interface and allow IP address swap during failover</b>	<p>Enables the network interface for the standby CMM and allows the IP addresses to swap between the two CMMs during failover.</p> <p><b>Note:</b> The <code>-ip swap</code> command option can not be run if only one CMM is installed in the chassis.</p>	<p><code>advfailover -ip swap</code></p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>                      where x is the primary CMM bay number.</p>
<b>Enable network interface and prevent IP address swap during failover</b>	<p>Enables the network interface for the standby CMM and prevents the IP addresses from swapping between the two CMMs during failover.</p> <p><b>Note:</b> The <code>-ip noswap</code> command option can not be run if only one CMM is installed in the chassis.</p>	<p><code>advfailover -ip noswap</code></p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>                      where x is the primary CMM bay number.</p>

### 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 385 for a list of error messages that apply to all commands or “airfilter command errors” on page 389 for a list of error messages that are specific to the airfilter command.

Table 7. *airfilter (set notification interval) command*

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display air filter change notification interval</b>	Displays the frequency of the chassis air filter reminder.	<code>airfilter</code>	Primary CMM:  <code>mm[p]</code> <code>mm[P]</code> <code>mm[x]</code> where <i>x</i> is the primary CMM bay number.
<b>Set air filter change notification interval</b>	Configures the frequency of the chassis air filter reminder. <b>Note:</b> 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.	<code>airfilter -freq frequency</code> where <i>frequency</i> is the interval, in months, between reminders to change the chassis air filter. Valid values are 0, 1, 3, and 6.  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"><li>• Supervisor</li><li>• Chassis account management</li><li>• Chassis log management</li><li>• Chassis administration</li><li>• Chassis configuration</li></ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  <code>mm[p]</code> <code>mm[P]</code> <code>mm[x]</code> where <i>x</i> is the primary CMM bay number.

**Example:** To view the current air filter notification interval, while the Flex System Enterprise 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 Flex System Enterprise 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>
```

---

## 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 385 for a list of error messages that apply to all commands or “alertcfg command errors” on page 389 for a list of error messages that are specific to the alertcfg command.

Table 8. *alertcfg* command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display global remote alert settings</b>	Displays the global remote alert settings for the CMM.	alertcfg	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Set remote alert retry delay interval</b>	Sets the remote alert retry delay interval.	alertcfg -dr <i>delay</i> -rl <i>limit</i> where <i>delay</i> 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.  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 8. alertcfg command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Include / exclude service information with email alerts</b>	Enables or disables inclusion of service information with email alerts.	<p>alertcfg -si state where state is enabled or disabled .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>
<b>Set remote alert retry limit</b>	Sets the maximum number of times the system will attempt to send a remote alert, if previous attempts were unsuccessful.	<p>alertcfg -rl value 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.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>

**Example:** To view the remote alert configuration, while the Flex System Enterprise 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 Flex System Enterprise 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
  
```

## 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 385 for a list of error messages that apply to all commands or “alertentries command errors” on page 389 for a list of error messages that are specific to the alertentries command.

Table 9. *alertentries command*

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



Table 9. *alertentries* command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<p><b>Delete alert recipient</b></p>	<p>Delete the specified alert recipient.</p>	<p><code>alertentries -recip_number-del</code>            where <i>recip_number</i> 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.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> <li>• Chassis log management</li> <li>• Chassis administration</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>
<p><b>Create alert recipient</b></p>	<p>Create the specified alert recipient. All fields must be specified when creating an alert recipient.</p>	<p><code>alertentries -recip_number-n recip_name -status alert_status-f filter_type-t notification_method -e email_addr</code>            where:</p> <ul style="list-style-type: none"> <li>• <i>recip_number</i> is a number from 1 to 12 that corresponds to an unused recipient number in the "Display alert properties for all recipients" list.</li> <li>• <i>recip_name</i> is a alphanumeric string up to 31 characters in length containing any character, including spaces, except for angle brackets (&lt; and &gt;). If the string includes spaces it must be enclosed in double-quotes.</li> <li>• <i>alert_status</i> is on or off for receipt of alerts.</li> <li>• <i>filter_type</i> filters the alert types received:</li> </ul>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>

Table 9. alertentries command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
		<p>critical (receive critical alerts only) or none (receive all alerts).</p> <ul style="list-style-type: none"> <li>• <i>notification_method</i> is email or snmp . <ul style="list-style-type: none"> <li>– For email , you must specify an email address (-e argument).</li> <li>– If snmp is selected, the -e argument is not needed.</li> </ul> </li> <li>• <i>email_addr</i> is a valid email address string up to 63 characters in length.</li> </ul> <p>(continued on next page)</p>	
<p><b>Create alert recipient</b> (continued)</p>		<p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> <li>• Chassis log management</li> <li>• Chassis administration</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	

Table 9. alertentries command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<p><b>Set alert recipient name</b></p>	<p>Sets a name for the specified alert recipient.</p>	<p>alertentries -<i>recip_number</i>-n <i>recip_name</i>            where:</p> <ul style="list-style-type: none"> <li>• <i>recip_number</i> is a number from 1 to 12 that corresponds to the recipient number assigned in the "Display alert properties for all recipients" list.</li> <li>• <i>recip_name</i> is a alphanumeric string up to 31 characters in length that can include any character, including spaces, except for angle brackets (&lt; and &gt;). If the name includes spaces, it must be enclosed in double-quotes.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> <li>• Chassis log management</li> <li>• Chassis administration</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>
<p><b>Set alert recipient status</b></p>	<p>Sets status for the specified alert recipient. The status determines if a recipient will receive alarm notifications.</p>	<p>alertentries -<i>recip_number</i>-status <i>alert_status</i>            where:</p> <ul style="list-style-type: none"> <li>• <i>recip_number</i> is a number from 1 to 12 that corresponds to the recipient number assigned in the "Display alert properties for all recipients" list.</li> <li>• <i>alert_status</i> is on or off.</li> </ul> <p>This command can only be run by users who have</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>

Table 9. *alertentries* command (continued)

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

Table 9. *alertentries* command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<p><b>Set alert notification method</b></p>	<p>Sets the alert notification method for the specified alert recipient.</p>	<p><code>alertentries -recip_ number -t notification_ method</code>            where:</p> <ul style="list-style-type: none"> <li>• <i>recip_number</i> is a number from 1 to 12 that corresponds to the recipient number assigned in the "Display alert properties for all recipients" list.</li> <li>• <i>notification_method</i> is               <ul style="list-style-type: none"> <li>- email</li> <li>- snmp</li> </ul> </li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> <li>• Chassis log management</li> <li>• Chassis administration</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>
<p><b>Set alert recipient email address</b></p>	<p>Sets the email address for the specified alert recipient. This email address is used to send alerts to the recipient via email. 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.</p>	<p><code>alertentries -recip_ number -e email_addr</code>            where:</p> <ul style="list-style-type: none"> <li>• <i>recip_number</i> is a number from 1 to 12 that corresponds to the recipient number assigned in the "Display alert properties for all recipients" list.</li> <li>• <i>email_addr</i> is a valid email address string up to 63 characters in length.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> </ul>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>

Table 9. alertentries command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
		<ul style="list-style-type: none"> <li>Chassis log management</li> <li>Chassis administration</li> <li>Chassis configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	
<b>Generate test alert</b>	Generates a test alert to verify correct alert response. <b>Notes:</b> <ul style="list-style-type: none"> <li>The <code>alertentries - test</code> command option must be used alone.</li> <li>If autoftp is enabled, sending a test alert will cause the system to send out service data as well.</li> </ul>	<b>alertentries - test</b> This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis account management</li> <li>Chassis log management</li> <li>Chassis administration</li> <li>Chassis configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.  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: <ul style="list-style-type: none"> <li>Chassis log management</li> <li>Chassis administration</li> <li>Blade administration</li> <li>Blade configuration</li> <li>Blade remote presence</li> <li>I/O module administration</li> <li>I/O module configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

**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@us.ibm.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@us.ibm.com
system:mm[1]> alertentries -2 -n test2 -status on -f critical -t email
-e test2@us.ibm.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 385 for a list of error messages that apply to all commands or “autoftp command errors” on page 390 for a list of error messages that are specific to the autoftp command.

Table 10. *autoftp* command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Display call-home settings for autoftp call home</b></p>	<p>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.</p>	<p><code>autoftp</code></p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where <i>x</i> is the primary CMM bay number.</p>
<p><b>Configure call-home settings for autoftp call home</b></p>	<p>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.</p> <p><b>Note:</b> The system will wait five days before sending duplicate events if they are left unacknowledged in the activity log.</p>	<p><code>autoftp -m mode -i ip_address -p port -u “user_name” -pw “password”</code>            where:</p> <ul style="list-style-type: none"> <li>• <i>mode</i> is one of the following automated problem reporting modes:               <ul style="list-style-type: none"> <li>– ftp</li> <li>– tftp</li> <li>– sftp</li> <li>– disabled</li> </ul> </li> <li>• <i>ip_address</i> is the IP address of the FTP, TFTP, or SFTP server</li> <li>• <i>port</i> 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.</li> <li>• “<i>user_name</i>” is the quote-delimited FTP or SFTP User Name for automated problem reporting (63 characters maximum).</li> <li>• “<i>password</i>” is the quote-delimited FTP or SFTP password for automated problem reporting (63 characters maximum).</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• For FTP and SFTP, all fields must be set.</li> <li>• For TFTP, only <code>-i</code> and <code>-p</code> are needed.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where <i>x</i> is the primary CMM bay number.</p>



### Example:

To view the settings of the automated call-home message feature, while the Flex System Enterprise 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.ibm.com over transmission port 69, while the Flex System Enterprise Chassis is set as the persistent command environment, at the `system >` prompt, type

```
autoftp -m tftp -i tftp.ibm.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.ibm.com
-p 6
-u smlite
system> autoftp -m tftp -i tftp.ibm.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 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 385 for a list of error messages that apply to all commands or “baydata command errors” on page 391 for a list of error messages that are specific to the baydata command.

Table 11. baydata command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Display bay data for all compute nodes</b></p>	<p>Displays compute node bay data for bay number, bay data status, and defined bay data for all bays.</p>	<p>baydata</p>	<p>Flex System Enterprise Chassis: system</p>
<p><b>Display compute node bay data for a specific bay</b></p>	<p>Displays the information assigned to the specified node bay. <b>Note:</b> 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.</p>	<p>baydata -b bay_num where bay_num :</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul> <p>The bay number must be within the scope assigned to the user. Valid subslot numbers are 1 and 2.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Flex System Enterprise Chassis: system</p>

Table 11. baydata command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Clear bay data</b>	Clears the node bay definition strings for all compute nodes bays within the user’s scope.	<p>baydata -clear</p> <p>The bay numbers must be within the scope assigned to the user.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	Flex System Enterprise Chassis:  system
<b>Clear bay data for specific bay</b>	<p>Clears the node bay definition strings for the specified node bay.</p> <p><b>Note:</b> 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.</p>	<p>baydata -b bay_num -clear</p> <p>where bay_num :</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul> <p>The bay number must be within the scope assigned to the user. Valid subslot numbers are 1 and 2.</p> <p>This command can only be run by users who have one or more of the</p>	Flex System Enterprise Chassis:  system

Table 11. baydata command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
		following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	
<b>Set bay data</b>	Sets node bay data for all compute nodes within the user's scope. This information can include: data about drivers or software, the Flex System Enterprise Chassis shelf number and IP address, and whether the compute node is a master or member in a high-availability system. <p><b>Note:</b> 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.</p>	baydata -data " <i>data_definition</i> " where " <i>data_definition</i> " is the ASCII string of up to 60 characters enclosed in double quotation marks - " <i>data_definition</i> ". The quotation marks are not stored. <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	Flex System Enterprise Chassis:  system

Table 11. baydata command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<p><b>Set node bay data definition for specific compute node</b></p>	<p>Sets node bay data for the specified compute node.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>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.</li> <li>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.</li> </ul> <p>If the command is issued to a specific bay, data is written to that compute node if it is in the user's scope.</p>	<p>baydata -b bay_num-data "data_definition"</p> <p>where:</p> <ul style="list-style-type: none"> <li>where "data_definition" is the quote-delimited ASCII string of up to 60 characters</li> <li>where bay_num : <ul style="list-style-type: none"> <li>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.</li> <li>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. The bay number must be within the scope assigned to the user. Valid subslot numbers are 1 and 2.</li> </ul> </li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Blade configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Flex System Enterprise Chassis:</p> <p>system</p>

**Example:** To view the bay data for all compute nodes, while the CMM is set as the persistent 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 Flex System Enterprise 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 385 for a list of error messages that apply to all commands or “bootmode command errors” on page 392 for a list of error messages that are specific to the bootmode command.

Table 12. bootmode command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display compute node boot mode</b>	Displays the boot mode settings of the specified compute node. <b>Note:</b> This command will execute only on compute nodes that support the bootmode feature.	bootmode	Compute node:  blade[x] where x is the node bay number.
<b>Set compute node boot mode</b>	Sets the copy of firmware that the specified compute node will use to boot: <ul style="list-style-type: none"> <li>• Temporary: booting from the temporary copy is recommended since it typically contains the latest enhancements and fixes.</li> <li>• Permanent: booting from the permanent copy should be used only when booting from the temporary copy is no longer possible.</li> </ul> Changes to the boot mode setting take effect after the next restart of the compute node. <b>Note:</b> This command will execute only on compute nodes that support the bootmode feature.	bootmode -p mode where mode is: <ul style="list-style-type: none"> <li>• temp for temporary firmware copy.</li> <li>• perm for permanent firmware copy.</li> </ul> This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Compute node:  blade[x] 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 Flex System Enterprise 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 385 for a list of error messages that apply to all commands or “bootseq command errors” on page 392 for a list of error messages that are specific to the bootseq command.

Table 13. *bootseq* command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display compute node boot sequence</b>	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.	<code>bootseq</code>	Compute node:  <code>blade[x]</code> where <i>x</i> is the node bay number.
<b>Set boot sequence for compute node</b>	Sets the boot sequence of the specified compute node. <b>Note:</b> The <code>-seq</code> option must be used exclusive of all other command options.	<code>bootseq -seq devicelist</code> where <i>devicelist</i> has one or more of the boot device IDs specified, as a pipe-separated ( ) list in order of preference.  A boot sequence of up to five boot devices can be specified and it can be seen by running the <code>bootseq</code> command with no options.  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Compute node:  <code>blade[x]</code> where <i>x</i> is the node bay number.
<b>Display information for boot device</b>	Displays settings for the specified boot device.	<code>bootseq -id ID</code> where <i>ID</i> is the boot device ID of the boot device.  Valid boot device IDs can be seen by running the <code>bootseq</code> command with no options.	Compute node:  <code>blade[x]</code> where <i>x</i> is the node bay number.



Table 13. *bootseq* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Set IP address for boot device (IPv4)</b></p>	<p>Sets IPv4 IP address information for specified boot device of the command target.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• A boot device must be specified using the <code>-id</code> command option.</li> <li>• Use the <code>-i</code>, <code>-g</code>, or <code>-s</code> options with no argument to clear the setting.</li> <li>• The host address, net mask, and gateway address must all be specified.</li> <li>• After IP address information is initially set, each option can be modified individually.</li> </ul>	<pre>bootseq -id device_id -i hostaddr -g netmask -s gateway</pre> <p>where:</p> <ul style="list-style-type: none"> <li>• <i>device_id</i> is a unique ID for the boot device.</li> <li>• <i>hostaddr</i> is the boot device IPv4 host address.</li> <li>• <i>netmask</i> is the boot device IPv4 netmask.</li> <li>• <i>gateway</i> is the boot device IPv4 gateway address.</li> </ul> <p>Valid boot device IDs can be seen by running the <code>bootseq</code> command with no options.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Compute node:</p> <p>blade[x] where x is the node bay number.</p>
<p><b>Clear IP address for boot device</b></p>	<p>Clears IP address information for specified boot device of the command target.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• A boot device must be specified using the <code>-id</code> command option.</li> <li>• The IP address options are cleared by entering no arguments.</li> <li>• The host address, net mask, and gateway address must all be cleared together.</li> </ul>	<pre>bootseq -id device_id -i -g -s</pre> <p>where <i>device_id</i> is a unique ID for the boot device.</p> <p>Valid boot device IDs can be seen by running the <code>bootseq</code> command with no options.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Compute node:</p> <p>blade[x] where x is the node bay number.</p>

**Example:** To display the boot sequence for the compute node in node bay 2, while the Flex System Enterprise 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 Flex System Enterprise 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 Flex System Enterprise 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 Flex System Enterprise 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 Flex System Enterprise 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 385 for a list of error messages that apply to all commands or “chconfig command errors” on page 393 for a list of error messages that are specific to the chconfig command.

Table 14. *chconfig* command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Display Service Advisor configuration</b></p>	<p>Displays the contact information for the Service Advisor feature. Service Advisor resides on your CMM and monitors your Flex System Enterprise 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 be opened, and a follow-up call will be made. This feature will generate a message to Lenovo when events occur in the Flex System Enterprise Chassis or one of its components that usually can be resolved without additional problem determination.</p> <p><b>Note:</b> The system will wait five days before sending duplicate events if they are left unacknowledged in the activity log.</p>	<p><code>chconfig</code></p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where <i>x</i> is the primary CMM bay number.</p>
<p><b>Display / accept Service Advisor terms and conditions</b></p>	<p>Displays or accepts the terms of the Service Advisor terms and conditions.</p>	<p><code>chconfig -li license</code> where <i>license</i> is</p> <ul style="list-style-type: none"> <li>• <code>view</code> to view the Service Advisor terms and conditions.</li> <li>• <code>accept</code> to accept the Service Advisor terms and conditions.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where <i>x</i> is the primary CMM bay number.</p>

Table 14. *chconfig* command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<p><b>Enable / disable Service Advisor terms and conditions</b></p>	<p>Enables or disables the call-home terms and conditions.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• All contact information fields are required before the Service Advisor can be enabled.</li> <li>• Call Home will connect to IBM through HTTPS and HTTP. HTTP Proxy fields must be set to permit for outbound traffic.</li> <li>• Service Advisor also needs to set up DNS server address on the CMM.</li> <li>• 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.</li> </ul>	<p><code>chconfig -sa <i>setting</i> -sc <i>support_center</i></code> where</p> <ul style="list-style-type: none"> <li>• <i>setting</i> is <ul style="list-style-type: none"> <li>– enable to activate the Service Advisor terms and conditions.</li> <li>– disable to suspend the Service Advisor terms and conditions.</li> </ul> </li> <li>• <i>support_center</i> is the 2character ISO 3166 country code of the Lenovo support center location. For example, the country code for the United States is US.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• Go to <a href="http://www.iso.org/iso/country_codes/iso_3166_code_lists/">http://www.iso.org/iso/country_codes/iso_3166_code_lists/</a> for a complete list of country codes.</li> <li>• Valid country codes must refer to countries that have Lenovo support centers.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>
<p><b>Set contact information for Service Advisor</b></p>	<p>Sets contact information for the Service Advisor.</p> <p><b>Note:</b> Each Service Advisor field can be set or updated independently, as well as specifying all fields at the same time, as shown here.</p>	<p><code>chconfig -co "<i>company</i>" -cn "<i>name</i>" -cph "<i>phone</i>" -cphe "<i>extension</i>" -ce <i>email</i> -mlph "<i>m_phone</i>" -ca "<i>address</i>" -cci "<i>city</i>" -cs <i>state</i> -sc <i>support_center</i> -cz "<i>postalcode</i>"</code> where:</p> <ul style="list-style-type: none"> <li>• "<i>company</i>" is the quote-delimited contact company</li> </ul>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>

Table 14. *chconfig* command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
		<p>name, of up to 30 characters in length.</p> <ul style="list-style-type: none"> <li>• <i>"name"</i> is the quote-delimited contact name, of 1 to 30 characters in length.</li> <li>• <i>"phone"</i> is the quote-delimited contact phone number, of 5 to 30 characters in length.</li> <li>• <i>"extension"</i> is the quote-delimited contact phone extension, of 1 to 30 characters in length.</li> <li>• <i>email</i> is email address of the contact person in the form <code>userid@hostname</code> (30 characters maximum). The <code>userid</code> can be alphanumeric characters, ".", "-", or "_" but must begin and end with alphanumeric characters. The <code>hostname</code> 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.</li> <li>• <i>"m_phone"</i> is the quote-delimited machine location phone number, of 5 to 30 characters in length.</li> </ul> <p><i>(continued on next page)</i></p>	
<p><b>Set contact information for Service Advisor</b> <i>(continued)</i></p>		<ul style="list-style-type: none"> <li>• <i>"address"</i> is the quote-delimited street address of the machine location, of 1 to 30 characters in length.</li> <li>• <i>"city"</i> is the quote-delimited city of the machine location, of 1</li> </ul>	

Table 14. *chconfig* command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
		<p>to 30 characters in length.</p> <ul style="list-style-type: none"> <li>• <i>state</i> is the state of the machine location, of 2 to 3 characters in length.</li> <li>• "<i>postalcode</i>" is the quote-delimited postal code of the machine location, of 1 to 9 alphanumeric characters in length.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	
<p><b>Set contact information for alternate Service Advisor</b></p>	<p>Sets contact information for an alternate Service Advisor.</p> <p><b>Note:</b> Each alternate Service Advisor field can be set or updated independently, as well as specifying all fields at the same time, as shown here.</p>	<p><code>chconfig -acn "<i>name</i>" -acph "<i>phone</i>" -acphe "<i>extension</i>" -ace <i>email</i> -mlph "<i>m_phone</i>" -ca "<i>address</i>" -cci "<i>city</i>" -cs <i>state</i> -sc <i>support_center</i> -cz "<i>postalcode</i>"</code>            where:</p> <ul style="list-style-type: none"> <li>• "<i>name</i>" is the quote-delimited contact name, of 1 to 30 characters in length.</li> <li>• "<i>phone</i>" is the quote-delimited contact phone number, of 5 to 30 characters in length.</li> <li>• "<i>extension</i>" is the quote-delimited contact phone extension, of 1 to 30 characters in length.</li> <li>• <i>email</i> is email address of the contact person in the form <code>userid@hostname</code> (30 characters maximum). The <code>userid</code> can be alphanumeric characters, ".", "-", or "_" but must begin and end with alphanumeric characters. The <code>hostname</code> can be</li> </ul>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where <i>x</i> is the primary CMM bay number.</p>

Table 14. *chconfig* command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
		<p>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.</p> <ul style="list-style-type: none"> <li>• "<i>m_phone</i>" is the quote-delimited machine location phone number, of 5 to 30 characters in length.</li> <li>• "<i>address</i>" is the quote-delimited street address of the machine location, of 1 to 30 characters in length.</li> </ul> <p>(continued on next page)</p>	
<p><b>Set contact information for alternate Service Advisor</b> (continued)</p>		<ul style="list-style-type: none"> <li>• "<i>city</i>" is the quote-delimited city of the machine location, of 1 to 30 characters in length.</li> <li>• <i>state</i> is the state of the machine location, of 2 to 3 characters in length.</li> <li>• "<i>postalcode</i>" is the quote-delimited postal code of the machine location, of 1 to 9 alphanumeric characters in length.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	



Table 14. *chconfig* command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<p><b>Set up HTTP proxy for Service Advisor</b></p>	<p>Sets up HTTP proxy for Service Advisor.</p>	<pre>chconfig -ps setting-loc hostname-po port-u "username"-pw "password"</pre> <p>where:</p> <ul style="list-style-type: none"> <li>• <i>setting</i> is enabled or disabled</li> <li>• <i>hostname</i> is the fully qualified host name or IP address of the HTTP proxy, of 1 to 63 characters in length.</li> <li>• <i>port</i> is the port of the HTTP proxy, a number from 1 to 65535, inclusive.</li> <li>• <i>"username"</i> is the quote-delimited user name, of 1 to 30 characters in length.</li> <li>• <i>"password"</i> is the quote-delimited password of the HTTP proxy, of up to 15 characters in length</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>

**Example:**

To accept the Service Advisor terms and conditions, while the Flex System Enterprise 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 Flex System Enterprise 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@cn.ibm.com
-cn bob
-co IBM
-cph 800-555-1111
-cs TX
-cz 75210
-cphe 5678
-acn mary
-acph 800-555-1113
-acphe 1234
-ace mary@cn.ibm.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 385 for a list of error messages that apply to all commands or “chlog command errors” on page 395 for a list of error messages that are specific to the chlog command.

Table 15. *chlog* (display call-home activity log) command

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Display call-home activity log entries</b>	<p>Displays the last fifty entries from the call-home activity log.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• The entries are displayed in reverse chronological order (most recent call-home entry first).</li> <li>• The system will wait 5 days before sending duplicate events if they are not acknowledged as corrected in the activity log.</li> <li>• Call-home events are usually those that can be resolved without additional problem determination.</li> </ul>	chlog	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>
<b>Display FTP/TFTP server call-home activity log entries</b>	<p>Displays the last fifty FTP/TFTP server entries from the call-home activity log.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• The entries are displayed in reverse chronological order (most recent call-home entry first).</li> <li>• The system will wait 5 days before sending duplicate events if they are not acknowledged as corrected in the activity log.</li> </ul>	chlog -f	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>

Table 15. *chlog* (display call-home activity log) command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display Lenovo Support call-home activity log entries</b>	<p>Displays the last five Lenovo Support entries from the call-home activity log.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>The entries are displayed in reverse chronological order (most recent call-home entry first).</li> <li>The system will wait 5 days before sending duplicate events if they are not acknowledged as corrected in the activity log.</li> <li>Call-home events are usually those that can be resolved without additional problem determination.</li> </ul>	<code>chlog -s</code>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>
<b>Acknowledge / unacknowledge call-home activity log entries</b>	<p>Marks the selected call-home event as acknowledged (yes) or unacknowledged (no) when the call-home event has been corrected.</p> <p><b>Note:</b> The system will wait five days before sending duplicate events if they are left unacknowledged in the activity log.</p>	<p><code>chlog -index-ack option</code> where:</p> <ul style="list-style-type: none"> <li><i>index</i> is the index of the call-home event entry</li> <li><i>option</i> is yes or no</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>

**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
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 Flex System Enterprise 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 385 for a list of error messages that apply to all commands or “chmanual command errors” on page 396 for a list of error messages that are specific to the chmanual command.

Table 16. *chmanual* command

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<p><b>Create call-home problem message</b></p>	<p>Create a call-home problem message for a CMM or compute node.</p>	<p><code>chmanual -desc "description"</code>            where "description" is a quote-delimited problem description of 1 to 100 characters in length.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> <li>• Chassis log management</li> <li>• Chassis administration</li> <li>• Chassis configuration</li> <li>• Blade administration</li> <li>• Blade configuration</li> <li>• Blade remote presence</li> <li>• I/O module administration</li> <li>• I/O module configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Flex System Enterprise Chassis:                system</p> <p>Compute node:                blade[x]            where x is the node bay number.</p>
<p><b>Generate call-home test call home</b></p>	<p>Manually generate a test call-home event that transmits the sample call-home problem message.</p>	<p><code>chmanual -test</code>            This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> <li>• Chassis log management</li> <li>• Chassis administration</li> <li>• Chassis configuration</li> <li>• Blade administration</li> <li>• Blade configuration</li> <li>• Blade remote presence</li> <li>• I/O module administration</li> <li>• I/O module configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Flex System Enterprise Chassis:                system</p>

**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 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 385 for a list of error messages that apply to all commands or “cimsub command errors” on page 396 for a list of error messages that are specific to the cimsub command.

Table 17. *cimsub* command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display CIM subscription destination</b>	Displays destinations for the CIM subscriptions used by the Flex System Manager software.	<code>cimsub</code>	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Display CIM subscription status</b>	Displays detailed information about all CIM subscriptions used by the Flex System Manager software.	<code>cimsub -v</code>	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Clear CIM subscription</b>	Clears one or all of the CIM subscriptions used by the Flex System Manager software.	<code>cimsub -clear identifier</code> where <i>identifier</i> is: <ul style="list-style-type: none"> <li>• all to delete all subscriptions.</li> <li>• a single destination URL identifier contained within double-quotes. Valid subscription identifiers can be seen by running the <code>cimsub</code> command with no arguments or the <code>cimsub -v</code> command.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

**Example:**

To display CIM destinations for the primary CMM, while the Flex System Enterprise 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 Flex System Enterprise 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 Flex System Enterprise 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 Flex System Enterprise 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_IndicationFilter\",Name=\"TEST:Indications:AllEvents\",SystemCreationClassName=\"CIM_ComputerSystem\",SystemName=\"\""
FailureTriggerTimeInterval = 3600
OnFatalErrorPolicy = 2
OtherRepeatNotificationPolicy = NULL
OtherSubscriptionState = NULL
RepeatNotificationCount = NULL
RepeatNotificationGap = NULL
RepeatNotificationInterval = NULL
RepeatNotificationPolicy = 2
SubscriptionDuration = NULL
SubscriptionState = 2
SubscriptionTimeRemaining = NULL
TimeOfLastStateChange = "20140212160444.680645-300"
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_IndicationFilter\",Name=\"TEST2:Indications:ALLEvents\",SystemCreationClassName=\"CIM_ComputerSystem\",SystemName=\"\"\"
FailureTriggerTimeInterval = 3600
OnFatalErrorPolicy = 2
OtherRepeatNotificationPolicy = NULL
OtherSubscriptionState = NULL
RepeatNotificationCount = NULL
RepeatNotificationGap = NULL
RepeatNotificationInterval = NULL
RepeatNotificationPolicy = 2
SubscriptionDuration = NULL
SubscriptionState = 2
SubscriptionTimeRemaining = NULL
TimeOfLastStateChange = "20140212160559.819293-300"
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> cimsu -clear "http://9.37.64.50:8080" -T mm[p]
OK
system> cimsu -clear all -T mm[p]
OK
system>
system> cimsu -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 385 for a list of error messages that apply to all commands or “cin command errors” on page 397 for a list of error messages that are specific to the cin command.

Table 18. cin command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display CIN configuration table</b>	<p>Displays the configuration table for the chassis internal network.</p> <p>Possible return values are:</p> <ul style="list-style-type: none"> <li>• Global CIN enabled or disabled status</li> <li>• CIN index               <ul style="list-style-type: none"> <li>– VLAN ID</li> <li>– IP address</li> <li>– index entry enabled or disabled status</li> </ul> </li> </ul>	cin	Flex System Enterprise Chassis:  system
<b>Set global CIN state</b>	Sets the global state of CIN to enabled or disabled.	<p>cin -global -en <i>state</i> where <i>state</i> is</p> <ul style="list-style-type: none"> <li>• on</li> <li>• off</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management and chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	Flex System Enterprise Chassis:  system
<b>Clear all CIN configuration entries</b>	Deletes all CIN configuration entries.	<p>cin all -clear</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management and chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	Flex System Enterprise Chassis:  system

Table 18. cin command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Turn all index entries on or off</b>	Turns all CIN index entries on or off.	<p>cin all -en <i>state</i>            where <i>state</i> is</p> <ul style="list-style-type: none"> <li>• on</li> <li>• off</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management and chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	Flex System Enterprise Chassis:  system
<b>Delete CIN configuration entry</b>	Deletes the specified CIN configuration entry.	<p>cin -<i>entry_index</i> -clear            where <i>entry_index</i> is a number between 1 and 14 (inclusive).</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management and chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	Flex System Enterprise Chassis:  system

Table 18. cin command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Set CIN configuration entry to enable or disable</b></p>	<p>Enables or disables a CIN configuration entry. If you attempt to enable or disable a non-existent entry, the action is ignored and no error message is returned.</p>	<p><code>cin -entry_index -en state</code> where:</p> <ul style="list-style-type: none"> <li>• <code>entry_index</code> is a number between 1 and 14, and</li> <li>• <code>state</code> is               <ul style="list-style-type: none"> <li>- on</li> <li>- off</li> </ul> </li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management and chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Flex System Enterprise Chassis: system</p>
<p><b>Create a CIN configuration entry</b></p>	<p>Creates a CIN index entry. If the CIN index is currently empty, both -id and -ip must be specified.</p> <p><b>Note:</b> The VLAN ID must be different from that of the compute nodeCMM.</p>	<p><code>cin -entry_index -id vlan_id -ip ip_address</code> where:</p> <ul style="list-style-type: none"> <li>• <code>entry_index</code> is a number between 1 and 14,</li> <li>• <code>vlan_id</code> is a VLAN ID number between 3 and 4094 (inclusive),</li> <li>• <code>ip_address</code> is a valid IP address.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management and chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Flex System Enterprise Chassis: system</p>

Table 18. cin command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Specify valid IP address for CIN index entry</b></p>	<p>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.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• If the index is not empty, the IP address can be specified separately.</li> <li>• CIN entries cannot have matching IP addresses unless they are 0.0.0.0. and have different VLAN IDs.</li> <li>• 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.</li> <li>• The IP address cannot be multi-cast and cannot match the IP address of the CMM.</li> </ul>	<p><code>cin -entry_index -ip ip_address</code>            where:</p> <ul style="list-style-type: none"> <li>• <i>entry_index</i> is a number between 1 and 14</li> <li>• <i>ip_address</i> is a valid IP address.</li> </ul> <p>You can overwrite parameters of an existing definition; for example, <code>cin -1 -ip 0.0.0.0</code> overwrites the current CIN IP address of the first cin entry. If the entry does not exist, an error is returned.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management and chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Flex System Enterprise Chassis:  system</p>
<p><b>Specify VLAN ID for CIN entry</b></p>	<p>Set the VLAN ID for the specified CIN entry.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• If the index is not empty, the ID can be specified separately.</li> <li>• The VLAN ID must be different from that of the CMM.</li> </ul>	<p><code>cin -entry_index -id vlan_id</code>            where:</p> <ul style="list-style-type: none"> <li>• <i>entry_index</i> is a number between 1 and 14</li> <li>• <i>vlan_id</i> is a number between 3 and 4094 (inclusive).</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management and chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Flex System Enterprise Chassis:  system</p>

### 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 385 for a list of error messages that apply to all commands or “cinstatus command errors” on page 398 for a list of error messages that are specific to the cinstatus command.

Table 19. cinstatus command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display entries of the CIN status table</b>	Reads entries of the CIN status table, five at a time. Each entry of the table returns: <ul style="list-style-type: none"><li>• CIN VLAN ID</li><li>• CIN IP address</li><li>• CIN MAC address</li><li>• CIN status text</li></ul> <b>Note:</b> An asterisk ( * ) shown next to an IP address indicates that it is a learned value.	cinstatus	Flex System Enterprise Chassis: system
<b>Display status of first five CIN entries</b>	Displays the first five entries of the CIN status table.	cinstatus -f	Flex System Enterprise Chassis: system
<b>Display entire CIN status table</b>	Displays all the entries in the CIN status table.	cinstatus -a	Flex System Enterprise Chassis: system

**Note:** An asterisk \* next to an IP address indicates a learned entry.

### Example:

To display five entries of the CIN status table, while the Flex System Enterprise 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      *00:00:00:00:00:00  Not Operational
2. 4094 0.0.0.2      *00:00:00:00:00:00  Not Operational
3. 4      0.0.0.0             00:00:00:00:00:00  Operational
4. 4093 0.0.0.1      *00:00:00:00:00:00  Not Operational
5. 4094 0.0.0.0             00:00:00:00:00:00  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 `-cfg` option.
- To restore a saved CMM configuration after restoring the manufacturing default settings, use the **read** command (see “read command” on page 269 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 385 for a list of error messages that apply to all commands or “clear command errors” on page 398 for a list of error messages that are specific to the clear command.

Table 20. clear command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Restore default configuration of primary CMM and keep logs</b></p>	<p>Restores the default configuration of the primary CMM, retaining log information; then, resets the CMM. If the current operating state of the Flex System Enterprise Chassis indicates potential problems with restoring the default configuration, an error message is returned and the restore is cancelled.</p> <p>No results are returned from this command because it resets the CMM.</p> <p>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 164 for information.</p>	<p>clear -cnfg</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis administration and chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>
<p><b>Restore default configuration of primary CMM and keep logs (with override)</b></p>	<p>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 Flex System Enterprise Chassis operating state.</p> <p>No results are returned from this command because it resets the CMM.</p> <p>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 164 for information.</p>	<p>clear -cnfg -o</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis administration and chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>

Table 20. `clear` command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Restore default configuration of I/O module</b>	Restores the configuration of the specified I/O module to the default settings.	<code>clear -cnfg</code> This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• I/O module administration and I/O module configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	I/O module:  <code>switch[x]</code> where <i>x</i> is the I/O-bay number.

**Example:** To restore the primary CMM configuration to default settings and retain log information, while the Flex System Enterprise 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 385 for a list of error messages that apply to all commands or “clearlog command errors” on page 399 for a list of error messages that are specific to the clearlog command.

Table 21. `clearlog` (clear CMM event log) command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Clear CMM event log</b></p>	<p>Clears the both the CMM audit event log and the CMM system event log, displaying a message confirming that both event logs were cleared.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• Audit log events are created by the actions of users.</li> <li>• 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.</li> <li>• 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.</li> </ul>	<p><code>clearlog</code></p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis log management</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where <code>x</code> is the primary CMM bay number.</p>
<p><b>Clear CMM audit or system event log</b></p>	<p>Clears the CMM audit event log, the system event log, or both, and displays a message confirming that the specified event log was cleared.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• Audit log events are created by the actions of users.</li> <li>• If the <code>log_type</code> is not specified, this command will clear both logs.</li> <li>• 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.</li> <li>• 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.</li> </ul>	<p><code>clearlog -l log_type</code>            where <code>log_type</code> is <code>audit</code> or <code>system</code> .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis log management</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where <code>x</code> is the primary CMM bay number.</p>

**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 : mm1 >` 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 385 for a list of error messages that apply to all commands or “config command errors” on page 399 for a list of error messages that are specific to the config command.

Table 22. config command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display identifying information for Flex System Enterprise Chassis</b>	Displays the following information for the command target: <ul style="list-style-type: none"> <li>Name</li> <li>Room</li> <li>Rack</li> <li>Rack unit</li> </ul>	config	Flex System Enterprise Chassis:  system
<b>Display name of compute node</b>	Displays the name of the specified compute node.	config	Compute node:  blade[x] where x is the node bay number.
<b>Display name of CMM</b>	Displays the following information for the command target: <ul style="list-style-type: none"> <li>Name</li> <li>Location</li> <li>Contact name</li> </ul>	config	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 22. config command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Set name of chassis</b>	Sets the name of the chassis.	<p>config -name "name" where "name" is up to 15 characters in length and contained within double-quotes. Any printable character can be used in the chassis name.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Flex System Enterprise Chassis:</p> <p style="padding-left: 40px;">system</p>
<b>Set name of CMM</b>	Sets the name of the primary CMM.	<p>config -name name where name is up to 15 characters in length.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration (for CMM)</li> <li>• Blade configuration (for compute node)</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p style="padding-left: 40px;">mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>

Table 22. config command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<p><b>Set name of compute node</b></p>	<p>Sets the name of the specified compute node.</p>	<p>config -name "name" where "name" is up to 15 characters in length and contained within double-quotes.</p> <p>Names can contain any character other than "&lt;" and "&gt;".</p> <p>Names can contain spaces.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Compute node:</p> <p>blade[x] where x is the node bay number.</p>
<p><b>Set rack location of chassis</b></p>	<p>Sets the rack where the chassis is located.</p>	<p>config -rack "rack" where "rack" is up to 23 characters in length and contained within double-quotes.</p> <p>Rack locations can contain any character other than "&lt;" and "&gt;".</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Flex System Enterprise Chassis:</p> <p>system</p>

Table 22. config command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Set rack unit location of chassis</b>	Sets the lowest rack unit that the chassis occupies in a rack.	<p>config -rackunit "<i>unit</i>" where "<i>unit</i>" is an integer between 0 and 99, inclusive, that identifies the lowest unit of a rack that the chassis occupies.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	Flex System Enterprise Chassis:  system
<b>Set room location of chassis</b>	Sets the room where the chassis is located.	<p>config -room "<i>room</i>" where "<i>room</i>" is up to 23 characters in length and contained within double-quotes.</p> <p>Room locations can contain any character other than "&lt;" and "&gt;".</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	Flex System Enterprise Chassis:  system



Table 22. *config* command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Set location of CMM</b>	Sets the location of the primary CMM.	<p><code>config -loc "location"</code> where "location" is up to 47 characters in length and contained within double-quotes.</p> <p>CMM locations can contain any character other than "&lt;" and "&gt;".</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>
<b>Set contact name for CMM</b>	Sets the contact name for the primary CMM.	<p><code>config -contact "contact_name"</code> where "contact_name" is up to 47 characters in length and contained within double-quotes.</p> <p>CMM contact names can contain any character other than "&lt;" and "&gt;".</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>

**Example:**

To set the primary CMM name to IBM\_lab, while the Flex System Enterprise Chassis is set as the persistent command environment, at the `system >` prompt, type

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

To display the primary CMM name, location, and contact name, while the Flex System Enterprise 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 IBM_Lab -T mm[p]
OK
system> config -T mm[p]
-name IBM_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 385 for a list of error messages that apply to all commands or “console command errors” on page 400 for a list of error messages that are specific to the console command.

Table 23. console command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Create SOL session with compute node</b>	Creates an SOL connection to the specified compute node. <b>Note:</b> 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.	<code>console</code> This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade remote presence</li> </ul> See “Commands and user authority” on page 10 for additional information.	Compute node:  <code>blade[x]</code> where <i>x</i> is the node bay number.
<b>Create override SOL session with compute node</b>	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. <b>Note:</b> The CMM supports combining this option with the <code>-l</code> option to override an existing session, and not reconnect if the connection drops.	<code>console -o</code> This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade remote presence</li> </ul> See “Commands and user authority” on page 10 for additional information.	Compute node:  <code>blade[x]</code> where <i>x</i> is the node bay number.
<b>Create non-persistent SOL session with compute node</b>	Creates an SOL connection to the specified compute node for users who do not want to use a persistent session. <b>Note:</b> This option can be combined with the <code>-o</code> option to override an existing session, and not reconnect if the connection drops.	<code>console -l</code> This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade remote presence</li> </ul> See “Commands and user authority” on page 10 for additional information.	Compute node:  <code>blade[x]</code> where <i>x</i> 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 Flex System Enterprise 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 112.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See “Common errors” on page 385 for a list of error messages that apply to all commands or “coolingzones command errors” on page 401 for a list of error messages that are specific to the coolingzones command.

Table 24. coolingzones command

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Display cooling zone information</b>	Display information for all cooling zones in the Flex System Enterprise Chassis.	coolingzones	Flex System Enterprise Chassis: system
<b>Display specific cooling zone information</b>	Displays detailed information for the specified cooling zone.	coolingzones z zone where zone is the cooling zone index number to display.  Valid cooling zone index numbers can be seen by running the coolingzones command with no argument.	Flex System Enterprise Chassis: 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 385 for a list of error messages that apply to all commands or “crypto command errors” on page 402 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 *Flex System Chassis Management Module User's Guide*.

Table 25. *crypto* command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display CMM cryptographic settings</b>	Displays the cryptographic settings for the CMM. Return values include the currently selected CMM cipher suite, cryptographic mode, and the cryptographic mode specification version.	<code>crypto</code>	Primary CMM:  <code>mm[p]</code> <code>mm[P]</code> <code>mm[x]</code> where <i>x</i> is the primary CMM bay number.
<b>Set CMM cipher suites</b>	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. <b>Important:</b> <ul style="list-style-type: none"><li>• If the <code>-cs</code> command option is run by itself, all secure connections are closed and will need to be reestablished after a successful cipher suite change.</li><li>• If the <code>-cs</code> and <code>-m</code> command options are run together, the CMM automatically restarts after a successful cipher suite and cryptographic mode change.</li></ul> <b>Notes:</b> <ul style="list-style-type: none"><li>• To set the cipher suite setting to <code>legacy</code>, the cryptographic mode must be set to <code>comp</code> (compatibility with all NIST cipher suites).</li><li>• The cipher suite cannot be changed from <code>tls1.2</code> to <code>tls1.2srv</code> when the cryptographic mode is set to <code>nist800-131a</code>.</li><li>• The cipher suite setting (<code>-cs</code>) is referred to as the TLS/SSL setting in the CMM Web interface (<b>Mgt Module Management &gt; Security &gt; Cryptography</b>).</li></ul>	<code>crypto -cs cipher</code> where <i>cipher</i> is: <ul style="list-style-type: none"><li>• <code>legacy</code> for legacy cryptographic settings (such as SSL)</li><li>• <code>tls1.2</code> for NIST Transport Layer Security (TLS) 1.2 cryptography on both the client and server</li><li>• <code>tls1.2srv</code> for NIST Transport Layer Security (TLS) 1.2 cryptography on only the server</li></ul> This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"><li>• Supervisor</li><li>• Chassis configuration</li></ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  <code>mm[p]</code> <code>mm[P]</code> <code>mm[x]</code> where <i>x</i> is the primary CMM bay number.
<b>Set CMM cryptographic mode</b>	Sets the cryptographic mode for the primary CMM. <b>Notes:</b> <ul style="list-style-type: none"><li>• To set the cryptographic mode to <code>nist800-131a</code>, the cipher suite setting must be set to <code>tls1.2</code> or <code>tls1.2srv</code>.</li><li>• If the <code>crypto -m</code> option is set to <code>comp</code> (compatibility with all NIST cipher suites), the <code>sslcfg -ca -csa</code></li></ul>	<code>crypto -m mode</code> where <i>mode</i> is: <ul style="list-style-type: none"><li>• <code>comp</code> for compatibility with all NIST cipher suites set by the <code>cipher -cs</code> command option.</li><li>• <code>nist800-131a</code> for compatibility with only the NIST Transport Layer Security (TLS) 1.2 cipher suites set by the <code>cipher -cs</code> command option.</li></ul>	Primary CMM:  <code>mm[p]</code> <code>mm[P]</code> <code>mm[x]</code> where <i>x</i> is the primary CMM bay number.

Table 25. `crypto` command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
	<p>option must be specified when generating a CA certificate (see the “<code>sslcfg</code> command” on page 317 for more information).</p> <ul style="list-style-type: none"> <li>• The CMM automatically restarts after a successful cryptographic mode change.</li> </ul>	<p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	

**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: mm1 >` 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: mm1 >` 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: mm1 >` 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 385 for a list of error messages that apply to all commands or “date command errors” on page 403 for a list of error messages that are specific to the date command.

Table 26. date command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display CMM clock information</b>	Displays the following information for the CMM clock: <ul style="list-style-type: none"> <li>• current date and time</li> <li>• GMT (Greenwich-Mean Time) offset</li> <li>• daylight-savings time setting</li> </ul>	date	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Display valid timezone settings</b>	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:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Display valid timezone settings (verbose)</b>	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. <b>Note:</b> The -v command option must be used with the date -tz all command option.	date -tz all -v	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.



Table 26. *date* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Set CMM date</b>	Sets the date for the CMM clock.	<p><code>date -d <i>date</i></code>            where <i>date</i> is the current calendar date in mm/dd/yyyy format.</p> <p>The month and day can be input as single digits. The year must be a four-digit number between 1970 and 2037 inclusive.</p> <p>This command can only be run by users who have the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Set CMM time</b>	Sets the time for the CMM clock.	<p><code>date -t <i>time</i></code>            where <i>time</i> is the current time in 24-hour hh:mm:ss format.</p> <p>The hours, minutes, and seconds can all be input as single digits.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Set CMM clock time zone</b>	Sets the time zone for the CMM clock. <b>Note:</b> The daylight-savings time setting for your time zone is set automatically.	<p><code>date -tz <i>timezone</i></code>            where <i>timezone</i> is one of the valid time zone values listed by the <code>date -tz all</code> command.</p> <p>This command can only be run by users who have the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	Primary CMM:  mm[p] mm[P] mm[x] 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 08/15/2013 and time of 10:38:00, while the Flex System Enterprise 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 08/15/2013
```

To display the clock information for the primary CMM, while the Flex System Enterprise 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 Flex System Enterprise 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 08/15/2013
OK
system> date -T mm[p]
08/15/2013 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 2014
system>
```

---

## dhcpcinfo 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 385 for a list of error messages that apply to all commands or “dhcpcinfo command errors” on page 404 for a list of error messages that are specific to the dhcpcinfo command.

Table 27. `dhcpcinfo` command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Display Ethernet channel 0 DHCP configuration for primaryCMM</b></p>	<p>If the IP configuration for the primaryCMM 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 <i>not</i> assigned by a DHCP server, an error message is displayed. Possible configuration values returned are:</p> <ul style="list-style-type: none"> <li>• <code>-server dhcp_ip_address</code></li> <li>• <code>-n hostname</code></li> <li>• <code>-i ip_address</code></li> <li>• <code>-g gateway_address</code></li> <li>• <code>-s subnet_mask</code></li> <li>• <code>-d domainname</code></li> <li>• <code>-dns1 primary_dns_ip_address</code></li> <li>• <code>-dns2 secondary_dns_ip_address</code></li> <li>• <code>-dns3 tertiary_dns_ip_1address</code></li> <li>• <code>-server6 IPv6_dhcp_ip_address</code></li> <li>• <code>-i6 IPv6_address</code></li> <li>• <code>-d6 IPv6_domainname</code></li> <li>• <code>-dns61 IPv6_primary_dns_ip_address</code></li> <li>• <code>-dns62 IPv6_secondary_dns_ip_address</code></li> <li>• <code>-dns63 IPv6_tertiary_dns_ip_1address</code></li> </ul>	<p><code>dhcpcinfo -eth0</code></p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where x is the primary CMM bay number.</p>
<p><b>Display Ethernet channel 0 DHCP configuration for standbyCMM</b></p>	<p>If the IP configuration for the standbyCMM 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 <i>not</i> assigned by a DHCP server, an error message is displayed. Possible configuration values returned are:</p> <ul style="list-style-type: none"> <li>• <code>-server dhcp_ip_address</code></li> <li>• <code>-n hostname</code></li> <li>• <code>-i ip_address</code></li> <li>• <code>-g gateway_address</code></li> <li>• <code>-s subnet_mask</code></li> <li>• <code>-d domainname</code></li> <li>• <code>-dns1 primary_dns_ip_address</code></li> <li>• <code>-dns2 secondary_dns_ip_address</code></li> <li>• <code>-dns3 tertiary_dns_ip_1address</code></li> <li>• <code>-server6 IPv6_dhcp_ip_address</code></li> <li>• <code>-i6 IPv6_address</code></li> <li>• <code>-d6 IPv6_domainname</code></li> <li>• <code>-dns61 IPv6_primary_dns_ip_address</code></li> </ul>	<p><code>dhcpcinfo -eth0 -standby</code></p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where x is the primary CMM bay number.</p>

Table 27. *dhcpcinfo* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
	<ul style="list-style-type: none"> <li>• -dns62 IPv6_secondary_dns_ip_address</li> <li>• -dns63 IPv6_tertiary_dns_ip_1address</li> </ul>		
<p><b>Display management network DHCP configuration for all compute node interfaces</b></p>	<p>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 <i>not</i> assigned by a DHCP server, an error message is displayed.</p> <p><b>Note:</b> 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 Flex System Manager hardware, if it is installed).</p>	<p>dhcpcinfo</p>	<p>Compute node:</p> <p>blade[x] where x is the node bay number.</p>

Table 27. `dhcpcfg` command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display management network DHCP configuration for specific compute node interface</b>	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 <i>not</i> assigned by a DHCP server, an error message is displayed.	<code>dhcpcfg -interface_label</code> where <i>interface_label</i> is any interface label reported by the compute node that specifies both the interface type and channel number. For example, <code>eth0</code> for Ethernet channel 0. Valid interface types include: <ul style="list-style-type: none"> <li>• <code>usb</code> for USB</li> <li>• <code>eth</code> for Ethernet</li> </ul> Valid interface types for a specific compute node can be seen by running the <code>dhcpcfg</code> command with no interface argument.	Compute node:  <code>blade[x]</code> where <i>x</i> is the node bay number.
<b>Display DHCP configuration for I/O module</b>	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 <i>not</i> assigned by a DHCP server, an error message is displayed.	<code>dhcpcfg</code>	I/O module:  <code>switch[x]</code> where <i>x</i> is the I/O-bay number.

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

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

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

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

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

```
system> dhcpcfg -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 *Flex System Enterprise Chassis Installation and Service Guide* 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 27.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See “Common errors” on page 385 for a list of error messages that apply to all commands or “displaylog command errors” on page 404 for a list of error messages that are specific to the displaylog command.

Table 28. `displaylog` (display CMM event log) command

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

Table 28. *displaylog* (display CMM event log) command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display log entries with auxiliary data</b>	Displays log entries with their auxiliary data.	<code>displaylog -aux</code>	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Display all event log filters</b>	Displays all filters that can be used to control CMM event log output.	<code>displaylog -filters</code>	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Display event log entries filtered by date</b>	Displays CMM event log information that meets the specified date filter criteria. <b>Notes:</b> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• 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.</li> </ul>	<code>displaylog -date date_filter</code> where <i>date_filter</i> is a pipe (   ) separated list of date filters in mm/dd/yy format.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.



Table 28. `displaylog` (display CMM event log) command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Display event log entries filtered by severity level</b></p>	<p>Displays CMM event log information that meets the specified severity level filter criteria.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• This command displays the first five most recent entries in the CMM event log that meet the specified filter criteria. Adding the <code>-a</code> option to the command displays all entries that meet the specified filter criteria.</li> <li>• 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.</li> <li>• 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.</li> </ul>	<p><code>displaylog -sev severity_filter</code>            where <i>severity_filter</i> is a pipe ( ) separated list of severity filters:</p> <ul style="list-style-type: none"> <li>• I (information)</li> <li>• E (error)</li> <li>• W (warning)</li> </ul>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where <i>x</i> is the primary CMM bay number.</p>
<p><b>Display event log entries filtered by every flag except the one specified</b></p>	<p>Displays CMM log information that is stored in logs other than the specified log.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• This command displays the first five most recent entries in the CMM event log that meet the specified filter criteria. Adding the <code>-a</code> option to the command displays all entries that meet the specified filter criteria.</li> <li>• 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.</li> <li>• 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.</li> </ul>	<p><code>displaylog -src ! filter_out</code>            where <i>filter_out</i> is the category of event log entries that is not to be displayed. Use the <code>displaylog -filters</code> command to discover excludable event log categories.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where <i>x</i> is the primary CMM bay number.</p>

Table 28. `displaylog` (display CMM event log) command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display audit log entries filtered by source</b>	<p>Displays CMM audit log information that meets the specified source filter criteria.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This command displays the first five most recent entries in the CMM event log that meet the specified filter criteria. Adding the <code>-a</code> option to the command displays all entries that meet the specified filter criteria.</li> <li>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.</li> <li>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.</li> </ul>	<p><code>displaylog -src source_filter</code>            where <code>source_filter</code> 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: <code>Blade_01-08</code>.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where <code>x</code> is the primary CMM bay number.</p>
<b>Display log entries filtered by call-home flag</b>	<p>Displays log entries that meet the specified call-home events filter criteria.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This command displays the five most recent entries in the CMM event log that meet the specified filter criteria. Adding the <code>-a</code> option to the command displays all entries that meet the specified filter criteria.</li> <li>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.</li> <li>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.</li> </ul>	<p><code>displaylog -ch option</code>            where <code>option</code> are:</p> <ul style="list-style-type: none"> <li>C (call home)</li> <li>N (non-serviceable)</li> <li>S (serviceable)</li> </ul>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where <code>x</code> is the primary CMM bay number.</p>
<b>Display the state of the log state event option</b>	<p>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.</p>	<p><code>displaylog -lse</code></p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where <code>x</code> is the primary CMM bay number.</p>

Table 28. `displaylog` (`display CMM event log`) command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Enable / disable monitoring of event log state</b>	Enables or disables the monitoring of the event log state to generate an event when the log becomes 75% or 100% full. <b>Note:</b> The <code>displaylog -lse</code> command must be run exclusive of other log-reading command options ( <code>-f</code> , <code>-a</code> , <code>-filters</code> , <code>-date</code> , <code>-sev</code> , <code>-src</code> , <code>-i</code> , and <code>-l</code> ).	<code>displaylog -lse state</code> where <code>state</code> is enabled or disabled .  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis log management</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where <code>x</code> is the primary CMM bay number.
<b>Save event log</b>	Saves the CMM event log to the specified location.	<code>displaylog -u URL</code> where <code>URL</code> is the fully qualified uniform resource locator, including file name, of the <code>tftp</code> , <code>ftp</code> , <code>http</code> , <code>https</code> , or <code>sftp</code> server where the event log is to be saved.	Primary CMM:  mm[p] mm[P] mm[x] where <code>x</code> 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 Flex System Enterprise 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 Flex System Enterprise 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 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 27.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See “Common errors” on page 385 for a list of error messages that apply to all commands or “displaysd command errors” on page 406 for a list of error messages that are specific to the displaysd command.

Table 29. displaysd command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display CMM connection and self-test status</b>	Displays connection status and latest self-test results for the primary CMM. <b>Note:</b> The displaysd -mmstat command must be run exclusive of other command options	displaysd -mmstat	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Save service information (with warnings)</b>	Saves service information from primary CMM to the specified location, displaying any warnings about standby CMM that might occur.	displaysd -u <i>URL</i> where <i>URL</i> 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:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Save service information (override warnings)</b>	Saves service information from primary CMM to the specified location, overriding warnings about standby CMM.	displaysd -u <i>URL</i> -o where <i>URL</i> 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:  mm[p] mm[P] mm[x] 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 385 for a list of error messages that apply to all commands or “dns command errors” on page 408 for a list of error messages that are specific to the dns command.

Table 30. dns command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display DNS configuration of CMM</b>	Displays the current DNS configuration of the CMM. Possible return values are: <ul style="list-style-type: none"> <li>• enabled</li> <li>• disabled</li> <li>• -i1 IPv4_first_ip_address</li> <li>• -i2 IPv4_second_ip_address</li> <li>• -i3 IPv4_third_ip_address</li> <li>• -i61 IPv6_first_ip_address</li> <li>• -i62 IPv6_second_ip_address</li> <li>• -i63 IPv6_third_ip_address</li> <li>• -ddns dynamic_DNS_state (enabled/disabled)</li> <li>• -p DNS_server_priority (ipv4/ipv6)</li> </ul>	dns	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>DNS - enable</b>	Enables the CMM DNS configuration. <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• At least one IP address must be non-zero to enable DNS.</li> <li>• 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.</li> </ul>	dns -on This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 30. dns command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>DNS - disable</b>	Disables the CMM DNS configuration. <b>Notes:</b> <ul style="list-style-type: none"> <li>• DNS lookup is always enabled.</li> <li>• When DHCP is in use, other DNS addresses might be assigned automatically by the DHCP server.</li> </ul>	dns -off This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Dynamic DNS - enable / disable</b>	Enables or disables dynamic DNS for the CMM.	dns -ddns <i>state</i> where <i>state</i> is enabled or disabled .  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>DNS first IPv4 IP address - set</b>	Sets the first IPv4 IP address. <b>Notes:</b> <ul style="list-style-type: none"> <li>• At least one IP address must be non-zero to enable DNS.</li> <li>• 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.</li> </ul>	dns -i1 <i>ip_address</i> where <i>ip_address</i> is the first IP address in dotted decimal IP address format.  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 30. dns command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>DNS second IPv4 IP address - set</b>	Sets the second IPv4 IP address. <b>Notes:</b> <ul style="list-style-type: none"> <li>At least one IP address must be non-zero to enable DNS.</li> <li>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.</li> </ul>	<code>dns -i2 ip_address</code> where <i>ip_address</i> is the second IP address in dotted decimal IP address format.  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  <code>mm[p]</code> <code>mm[P]</code> <code>mm[x]</code> where <i>x</i> is the primary CMM bay number.
<b>DNS third IPv4 IP address - set</b>	Sets the third IPv4 IP address. <b>Notes:</b> <ul style="list-style-type: none"> <li>At least one IP address must be non-zero to enable DNS.</li> <li>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.</li> </ul>	<code>dns -i3 ip_address</code> where <i>ip_address</i> is the third IP address in dotted decimal IP address format.  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  <code>mm[p]</code> <code>mm[P]</code> <code>mm[x]</code> where <i>x</i> is the primary CMM bay number.
<b>DNS first IPv6 IP address - set</b>	Sets the first IPv6 IP address. <b>Notes:</b> <ul style="list-style-type: none"> <li>At least one IP address must be non-zero to enable DNS.</li> <li>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.</li> </ul>	<code>dns -i61 ip_address</code> where <i>ip_address</i> is the first IP address in IPv6 format.  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  <code>mm[p]</code> <code>mm[P]</code> <code>mm[x]</code> where <i>x</i> is the primary CMM bay number.



Table 30. dns command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>DNS second IPv6 IP address - set</b>	<p>Sets the second IPv6 IP address.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>At least one IP address must be non-zero to enable DNS.</li> <li>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.</li> </ul>	<p><code>dns -i62 ip_address</code>                      where <i>ip_address</i> is the second IP address in IPv6 format.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]                      mm[P]                      mm[x]                      where x is the primary CMM bay number.</p>
<b>DNS third IPv6 IP address - set</b>	<p>Sets the third IPv6 IP address.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>At least one IP address must be non-zero to enable DNS.</li> <li>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.</li> </ul>	<p><code>dns -i63 ip_address</code>                      where <i>ip_address</i> is the third IP address in IPv6 format.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]                      mm[P]                      mm[x]                      where x is the primary CMM bay number.</p>
<b>DNS server priority - set</b>	<p>Sets the DNS server priority for the CMM to IPv4 or IPv6..</p>	<p><code>dns -p priority</code>                      where <i>priority</i> is <code>ipv4</code> or <code>ipv6</code> .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]                      mm[P]                      mm[x]                      where x is the primary CMM bay number.</p>

**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 Flex System Enterprise 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 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 and IBM systems.

**Note:** To see installed targets for your Flex System Enterprise Chassis, use the “list command” on page 214.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See “Common errors” on page 385 for a list of error messages that apply to all commands or “env command errors” on page 408 for a list of error messages that are specific to the `env` command.

Table 31. env command

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Set Flex System Enterprise Chassis as command target</b>	Sets the Flex System Enterprise 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 <code>system &gt;</code> prompt.	<code>env</code> <code>env -T system</code>	The env command can be directed to any installed device.
<b>Set CMM as command target</b>	Sets the CMM as the persistent target for commands during the current session.	<code>env -T system:mm [x]</code> where <i>x</i> is the bay (1 or 2) that identifies the CMM.	The env command can be directed to any installed device, in this case <code>mm[x]</code> where <i>x</i> is the CMM bay number.
<b>Set primary CMM as command target</b>	Sets the primary CMM as the persistent target for commands during the current session.	<code>env -T system:mm[p]</code> <code>env -T system:mm[P]</code>	The env command can be directed to any installed device, in this case <code>mm[p]</code> <code>mm[P]</code>
<b>Set standby CMM as command target</b>	Sets the standby CMM as the persistent target for commands during the current session.	<code>env -T system:mm[s]</code> <code>env -T system:mm[S]</code>	The env command can be directed to any installed device, in this case <code>mm[s]</code> <code>mm[S]</code>
<b>Set compute node as command target</b>	Sets the specified compute node as the persistent target for commands during the current session.	<code>env -T system:blade [x]</code> where <i>x</i> 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 <code>blade[x]</code> where <i>x</i> is the node bay that identifies the compute node.
<b>Set logical node grouping as command target</b>	Sets the logical node grouping as the persistent target for commands during the current session.	<code>env -T system:bladegroup [x]</code> where <i>x</i> 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 <code>bladegroup[x]</code>  where <i>x</i> is the node bay that identifies the logical node grouping.

Table 31. env command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Set compute node in logical node grouping as command target</b></p>	<p>Sets the specified compute node in a logical node grouping as the persistent target for commands during the current session.</p> <p><b>Note:</b> When a compute node is part of a logical node grouping, syntax for compute node sub-components is of the form: <code>env -T system:bladegroup[x]:blade[y]:comp</code>, as discussed in Set compute node sub-component as command target</p>	<p><code>env -T system:bladegroup[x]:blade[y]</code>            where:</p> <ul style="list-style-type: none"> <li>• <code>x</code> 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.</li> <li>• <code>y</code> is the identifier for the compute node in the logical node grouping.</li> </ul>	<p>The env command can be directed to any installed device, in this case <code>bladegroup[x]:blade[y]</code>            where:</p> <ul style="list-style-type: none"> <li>• <code>x</code> 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.</li> <li>• <code>y</code> is the identifier for the compute node in the logical node grouping.</li> </ul>
<p><b>Set compute node sub-component as command target</b></p>	<p>Sets the specified sub-component on the specified compute node as the persistent target for commands during the current session. Valid sub-components are:</p> <ul style="list-style-type: none"> <li>• Node system-management processor</li> <li>• Expansion adapter</li> <li>• Add-in card</li> <li>• Add-in card PCI-Express module</li> <li>• Microprocessor</li> <li>• Expansion node</li> <li>• High-speed expansion card</li> <li>• Memory</li> <li>• Flash DIMM storage (Lenovo eXFlash Storage DIMM)</li> <li>• Storage backplane</li> <li>• Alarm panel</li> </ul>	<p><code>env -T system:blade [x]:comp</code>            where <code>x</code> 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.</p> <p>where <code>comp</code> is the sub-component:</p> <ul style="list-style-type: none"> <li>• <code>sp</code> for node system-management processor</li> <li>• <code>exp [x]</code> for expansion adapter (where <code>x</code> identifies the expansion adapter)</li> <li>• <code>cpu [x]</code> for microprocessor (where <code>x</code> identifies the microprocessor)</li> <li>• <code>addin [x]</code> for add-in card (where <code>x</code> identifies the add-in card)</li> <li>• <code>pciexpress [x]</code> for add-in card PCI-Express module (where <code>x</code> identifies the PCI-Express module)</li> </ul>	<p>The env command can be directed to any installed device, in this case <code>blade[x]:comp</code>            where <code>x</code> is the node bay that identifies the compute node on which the sub-component is installed.</p> <p>where <code>comp</code> is the sub-component:</p> <ul style="list-style-type: none"> <li>• <code>sp</code> for node system-management processor</li> <li>• <code>exp [x]</code> for expansion adapter (where <code>x</code> identifies the expansion adapter)</li> <li>• <code>cpu [x]</code> for microprocessor (where <code>x</code> identifies the microprocessor)</li> <li>• <code>addin [x]</code> for add-in card (where <code>x</code> identifies the add-in card)</li> <li>• <code>pciexpress [x]</code> for add-in card PCI-Express module</li> </ul>

Table 31. env command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
		<ul style="list-style-type: none"> <li>• stgbkplane [x] for storage backplane card (where x identifies the storage backplane)</li> <li>• be [x] for expansion node (where x identifies the expansion node)</li> <li>• hsec [x] for high-speed expansion card (where x identifies the high-speed expansion card)</li> <li>• memory [x] for memory (where x identifies the memory module)</li> <li>• flashdim [x] for flash DIMM (where x identifies the flash DIMM storage module)</li> </ul> <p>(continued on next page)</p>	<ul style="list-style-type: none"> <li>(where x identifies the PCI-Express module)</li> <li>• be [x] for expansion node (where x identifies the expansion node)</li> <li>• stgbkplane [x] for add-in card (where x identifies the storage backplane)</li> <li>• hsec [x] for high-speed expansion card (where x identifies the high-speed expansion card)</li> <li>• memory [x] for memory (where x identifies the memory module)</li> </ul> <p>(continued on next page)</p>
<p><b>Set compute node sub-component as command target</b> (continued)</p>		<ul style="list-style-type: none"> <li>• mgmtcrd [x] for management card (where x identifies the management card)</li> <li>• tap [x] for alarm panel (where x identifies the alarm panel)</li> </ul>	<ul style="list-style-type: none"> <li>• flashdim [x] for flash DIMM (where x identifies the flash DIMM storage module)</li> <li>• mgmtcrd [x] for management card (where x identifies the management card)</li> <li>• tap [x] for alarm panel (where x identifies the alarm panel)</li> </ul>
<p><b>Set I/O module as command target</b></p>	<p>Sets the specified I/O module as the persistent target for commands during the current session.</p>	<p>env -T system:switch [x] where x is the I/O bay where the I/O module is installed.</p>	<p>The env command can be directed to any installed device, in this case switch[x] where x is the I/O bay where the I/O module is installed.</p>

Table 31. env command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Set power supply as command target</b>	Sets the specified power supply as the persistent target for commands during the current session.	<code>env -T system:power [x]</code> where <i>x</i> is the power supply bay where the power supply is installed.	The env command can be directed to any installed device, in this case <code>power[x]</code> where <i>x</i> is the power supply bay where the power supply is installed.
<b>Set fan logic module as command target</b>	Sets the specified fan logic module as the persistent target for commands during the current session.	<code>env -T system:fanmux [x]</code> where <i>x</i> is the bay where the fan logic module is installed.	The env command can be directed to any installed device, in this case <code>fanmux[x]</code> where <i>x</i> is the bay where the fan logic module is installed.
<b>Set fan module as command target</b>	Sets the specified fan module as the persistent target for commands during the current session.	<code>env -T system:blower [x]</code> where <i>x</i> is the fan module bay where the fan module is installed.	The env command can be directed to any installed device, in this case <code>blower[x]</code> where <i>x</i> is the fan module bay where the fan module is installed.
<b>Set rear LED card as command target</b>	Sets the rear LED card as the persistent target for commands during the current session.	<code>env -T system:mt [x]</code> where <i>x</i> is the rear LED card.	The env command can be directed to any installed device, in this case <code>mt[x]</code>  where <i>x</i> is the rear LED card.
<b>Set storage expansion enclosure as command target</b>	Sets the storage expansion enclosure as the persistent target for commands during the current session.	<code>env -T system:bladeenclosure [x]</code> where <i>x</i> 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 <code>bladeenclosure[x]</code>  where <i>x</i> 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 Flex System Enterprise 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 Flex System Enterprise 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 385 for a list of error messages that apply to all commands or “ethoverusb command errors” on page 408 for a list of error messages that are specific to the ethoverusb command.

Table 32. ethoverusb command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display compute node Ethernet-over-USB setting</b>	Displays the Ethernet-over-USB command interface setting for the system-management processor of the specified compute node. <b>Note:</b> 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:  blade[x] where x is the node bay number.
<b>Set compute node Ethernet-over-USB setting</b>	Enables or disables the Ethernet-over-USB command interface setting for the system-management processor of the specified compute node. <b>Notes:</b> <ul style="list-style-type: none"> <li>This command will execute only on compute nodes that support an Ethernet-over-USB command interface for the node system-management processor.</li> <li>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.</li> </ul>	ethoverusb -s <i>state</i> where <i>state</i> is enabled or disabled .  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>Supervisor</li> <li>Blade administration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Compute node:  blade[x] 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 385 for a list of error messages that apply to all commands or “events command errors” on page 409 for a list of error messages that are specific to the events command.

Table 33. *events* command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display Call Home events list and free space</b>	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.	<p><code>events -che</code></p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> <li>• Chassis log management</li> <li>• Chassis administration</li> <li>• Chassis configuration</li> <li>• Blade administration</li> <li>• Blade configuration</li> <li>• Blade remote presence</li> <li>• I/O module administration</li> <li>• I/O module configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where <i>x</i> is the primary CMM bay number.</p>
<b>Add a Call Home event to the Call Home Exclusion list</b>	<p>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.</p> <p><b>Note:</b> 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.</p>	<p><code>events -che -add event_ID</code>            where <i>event_ID</i> is an eight-digit hexadecimal number with an optional prefix of 0x or 0X.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where <i>x</i> is the primary CMM bay number.</p>
<b>Remove a Call Home event from the Call Home Exclusion list</b>	<p>Removes a Call Home event from the Call Home exclusion list. Events removed from this list are included in the Call Home reports.</p> <p><b>Note:</b> 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.</p>	<p><code>events -che -rm event_ID</code>            where <i>event_ID</i> is</p> <ul style="list-style-type: none"> <li>• an eight-digit hexadecimal number with an optional prefix of 0x or 0X to remove a single Call Home event</li> <li>• all to remove all the Call Home events from the exclusion list</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where <i>x</i> is the primary CMM bay number.</p>

**Example:** To view the Call Home exclusion list and the number of remaining events can be added to the list, while the Flex System Enterprise 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 Flex System Enterprise 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 Flex System Enterprise 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 385 for a list of error messages that apply to all commands or “exit command errors” on page 409 for a list of error messages that are specific to the exit command.

Table 34. *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 <b>Note:</b> 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 385 for a list of error messages that apply to all commands or “files command errors” on page 410 for a list of error messages that are specific to the files command.

Table 35. files command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display file list and free space</b>	Displays a list of files and space remaining in the CMM file system.	files	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Delete file</b>	Deletes a file from the CMM file system. <b>Note:</b> This command can only be used to delete files: it will not delete directories.	files -d <i>filename</i> where <i>filename</i> is a valid, existing filename of less than 256 characters in length.  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis administration</li> <li>• Chassis configuration</li> <li>• Blade administration</li> <li>• Blade configuration</li> <li>• I/O module administration</li> <li>• I/O module configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

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

To delete the file **tftpboot/tftp\_file.pkt** from the primary CMM file system, while the Flex System Enterprise Chassis is set as the persistent command environment, at the **system >** prompt, type  
 files -d tftpboot/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 2006 lost+found/
1024 Thu Jul 06 19:32:51 2006 tftproot/
1024 Thu Jul 06 19:34:15 2006 tftproot/test/
1024 Thu Jul 06 19:34:15 2006 tftproot/test/test2/
0 Sat Aug 19 09:22:02 2006 tftproot/tftp_file.pkt
0 Sun Oct 01 07:57:19 2006 tftproot/.Do_not_delete_this_directory
0 Tue Dec 15 11:07:19 2009 test
0 Thu Apr 13 23:45:40 2006 bob.pkt
1024 Tue Feb 02 15:29:17 2010 pubkeys/
426 Tue Feb 02 15:29:17 2010 pubkeys/ssh_key.pub
5652 Fri May 12 00:56:36 2006 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 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 Flex System Manager management server is installed in the Flex System Enterprise Chassis, you can activate the Features on Demand features for compute node firmware using the Flex System Manager 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 385 for a list of error messages that apply to all commands or “fod command errors” on page 410 for a list of error messages that are specific to the fod command.

Table 36. fod command

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

**Example:** To view the feature license information for the primary CMM in bay 1, while the Flex System Enterprise 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

Open Fabric Manager
  Index: 1
  Status: Valid
  Description: SYSTEM X FEATURE ON DEMAND ACTIVATION KEY
  Size: 412 bytes
  System: IBM Flex Chassis
  Identifier: MTSN 872123DVG73
  Feature: Open Fabric Manager
  Feature Type: 0014
  Activation Expiration: Thu Sep 10 04:59:59 2015
  Validation: SHA-1 RSA 2048
system>
```

---

## fruactlog command

This command displays a summary of the hardware activity for modules installed in the Flex System Enterprise 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 385 for a list of error messages that apply to all commands or “fruactlog command errors” on page 411 for a list of error messages that are specific to the fruactlog command.

Table 37. fruactlog command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display chassis activity summary</b>	Displays a list of hardware activity for chassis modules, along with their VPD information.	fruactlog	Flex System Enterprise Chassis: system

**Example:** To view the list of chassis module activity and VPD information, while the Flex System Enterprise 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: IBM  
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: IBM  
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: IBM  
Time/Date: 09/25/12, 13:59:07  
Action: Inserted
```

```
.  
. .  
. . .
```

```
system>
```

---

## fsmcm command

This command disables centralized user account management from the optional 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 385 for a list of error messages that apply to all commands or “fsmcm command errors” on page 411 for a list of error messages that are specific to the fsmcm command.

Table 38. fsmcm (disable centralized account management) command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Disable centralized user account management</b></p>	<p>Disables centralized account management, allowing use of local CMM user accounts.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• Centralized user account management is enabled by the optional Flex System Manager management software.</li> <li>• When centralized user account management is enabled by the optional Flex System Manager management software: <ul style="list-style-type: none"> <li>– 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.</li> <li>– Users logged in to the CMM web interface and CLI are logged out when their user accounts are disabled.</li> </ul> </li> <li>• When running the fsmcm -off command using the Flex System Manager management software created recovery account (RECOVERY_ID): <ul style="list-style-type: none"> <li>– 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.</li> <li>– The RECOVERY_ID user account is deleted.</li> <li>– 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 353).</li> </ul> </li> <li>• See the Flex System Manager documentation for information about accessing the CMM after centralized user account management is enabled.</li> </ul>	<p>fsmcm -off</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>

**Example:** To disable centralized user account management when logged in using the RECOVERY\_ID user account, while the Flex System Enterprise 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 Flex System Enterprise 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 385 for a list of error messages that apply to all commands or “fuelg command errors” on page 411 for a list of error messages that are specific to the fuelg command.

Table 39. fuelg command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display power domain status overview</b>	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. <b>Note:</b> 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	Flex System Enterprise Chassis:  system
<b>Display compute node power status overview</b>	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: <ul style="list-style-type: none"> <li>• CPU duty cycles</li> <li>• Effective and maximum CPU speeds</li> <li>• Power capping value (minimum and maximum)</li> <li>• Maximum, minimum, and average power levels</li> <li>• Time when above data was captured</li> <li>• Power saver mode status (on, off)</li> </ul>	fuelg	Compute node:  blade[x] where x is the node bay number.

Table 39. fuelg command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display I/O module power status</b>	Displays the maximum, minimum, and average power information for the specified I/O module.	fuelg	I/O module:  switch[x] where x is the I/O-bay number.
<b>Display fan module power status and temperature</b>	Displays the maximum power, minimum power, average power, and current temperature information for the specified fan module.	fuelg	Fan module:  blower[x] where x is the fan module bay number.
<b>Display rear LED card temperature</b>	Displays the minimum, maximum, and average temperature for the specified rear LED card.	fuelg	Rear LED card:  mt[x] where x is the rear LED card.
<b>Display detailed power domain status</b>	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: <ul style="list-style-type: none"> <li>• * - compute node might throttle</li> <li>• C - communication error</li> <li>• D - discovering</li> <li>• Hib - hibernate</li> <li>• NP - module is not present</li> <li>• SB - standby</li> <li>• T - throttled</li> <li>• U - unable to power up</li> </ul> <b>Note:</b> The Flex System Enterprise Chassis has only one power domain.	fuelg pd	Flex System Enterprise Chassis:  system

Table 39. *fuelg* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Set power domain redundancy loss policy</b></p>	<p>Sets how the Flex System Enterprise Chassis responds to a condition that could cause a loss of redundant power.</p>	<p><i>fuelg pd -pm policy</i> where <i>policy</i> is:</p> <ul style="list-style-type: none"> <li>• <i>acred</i> (ac power source redundancy policy)</li> <li>• <i>acredov</i> (ac power source redundancy policy, with compute node throttling)</li> <li>• <i>redwoperf</i> (power module redundancy, no compute node oversubscription)</li> <li>• <i>redwperf</i> (power module redundancy with compute node power throttling)</li> <li>• <i>nonred</i> (no power management policy)</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Flex System Enterprise Chassis:  system</p>
<p><b>Display power trending for specified time period for power domain</b></p>	<p>Displays power trending information, for the selected time interval, for the power domain of the Flex System Enterprise Chassis. <b>Note:</b> The Flex System Enterprise Chassis has only one power domain.</p>	<p><i>fuelg pd -pt period</i> where <i>period</i> is 1, 6, 12, or 24 hours.</p>	<p>Flex System Enterprise Chassis:  system</p>

Table 39. *fuelg* command (continued)

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

Table 39. *fuelg* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Set hot air recirculation detection state</b>	Enables or disables hot air recirculation detection for the Flex System Enterprise Chassis.	<p><i>fuelg</i> -har <i>setting</i>            where a <i>setting</i> of:</p> <ul style="list-style-type: none"> <li>• disabled turns off hot air recirculation detection for the chassis.</li> <li>• enabled (default) turns on hot air recirculation detection for the chassis.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	Flex System Enterprise Chassis:  system
<b>Set hot air recirculation threshold</b>	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.	<p><i>fuelg</i> -hart <i>setting</i>            where <i>setting</i> 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.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	Flex System Enterprise Chassis:  system
<b>Display air flow trending for specified time period</b>	Displays chassis air flow trending information, in cubic feet per minute (CFM), for the selected time interval.	<i>fuelg</i> -aft <i>period</i> where <i>period</i> is 1, 6, 12, or 24 hours.	Flex System Enterprise Chassis:  system

Table 39. *fuelg* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Thermal event response</b> (acoustic mode)</p>	<p>Sets the acoustic mode of Flex System Enterprise Chassis fan system response to thermal events.</p>	<p><i>fuelg -am setting</i> where the acoustic-mode <i>setting</i> is <i>off</i> or a number from 1 to 5, inclusive. A value of <i>off</i> 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.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Flex System Enterprise Chassis:  system</p>
<p><b>Set static power limit</b></p>	<p>Sets the static power limit value for the Flex System Enterprise Chassis. <b>Note:</b> To set the static power limit value for the chassis, power management and capping for the chassis must <i>not</i> be set to none (<i>fuelg -pme static</i>).</p>	<p><i>fuelg -spl setting</i> where <i>setting</i> is:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• a maximum wattage value, indicated by <i>w</i>, 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.</li> </ul> <p>Available power for a chassis is displayed by running the <i>fuelg</i> command, with no options, on the <i>system</i> target.</p>	<p>Flex System Enterprise Chassis:  system</p>

Table 39. *fuelg* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
		<p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	
<p><b>Set power capping value</b></p>	<p>Sets the power capping value for the specified command target that supports this feature.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• Setting a power capping value for a compute node, automatically turns on power management and capping for the compute node (<i>fuelg -pme on</i>).</li> <li>• A compute node must be turned on before you can set its power capping value.</li> <li>• When setting <i>-pcap</i> 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 <i>fuelg</i> command with no options to see the amount of power currently allocated.</li> <li>• Reconfiguration of the <i>fuelg -pcap</i> value might be required when disabling <i>fuelg -dps</i> to make sure that the power allocated for a node is not greater than the maximum power limit allowed.</li> </ul>	<p><i>fuelg -pcap setting</i> where <i>setting</i> is a numeric wattage value that falls within the range of power capping values displayed when running the <i>fuelg</i> command, with no options, on the target.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Compute node:</p> <p>blade[x] where x is the node bay number.</p>

Table 39. *fuelg* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Power management and capping - enable or disable</b></p>	<p>Turns power management and capping for the specified command target on or off.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• If power management and capping is set to static for a chassis, you must also specify a static power limit value (<i>fuelg -spl value</i>).</li> <li>• A compute node must be turned on before you can enable power management and capping for it.</li> </ul>	<p><i>fuelg -pme setting</i> where:</p> <ul style="list-style-type: none"> <li>• for the chassis target, a <i>setting</i> of: <ul style="list-style-type: none"> <li>– none (default) disables power management and capping for the chassis.</li> <li>– static enables power management and capping for the chassis.</li> </ul> </li> <li>• for a compute node target, a <i>setting</i> of: <ul style="list-style-type: none"> <li>– off (default) disables power management and capping for the compute node.</li> <li>– on enables power management and capping for the compute node.</li> </ul> </li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Flex System Enterprise Chassis:</p> <p>system</p> <p>Compute node:</p> <p>blade[x] where x is the node bay number.</p>
<p><b>Static low power saver mode - enable or disable for compute node</b></p>	<p>Turns the static low power saver mode for the specified compute node on or off.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• A compute node must be turned on before you can enable power saver mode for it.</li> <li>• Not all compute nodes support the power saver mode.</li> </ul>	<p><i>fuelg -ps setting</i> where a <i>setting</i> of:</p> <ul style="list-style-type: none"> <li>• off (default) disables power saver mode for the compute node.</li> <li>• on enables power saver mode for the compute node.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Compute node:</p> <p>blade[x] where x is the node bay number.</p>



Table 39. *fuelg* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Dynamic power optimizer - enable or disable for compute node</b></p>	<p>Turns dynamic power optimizer for the specified compute node on or off.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• A compute node must be turned on before you can enable dynamic power optimizer for it.</li> <li>• Not all compute nodes support the dynamic power optimizer.</li> <li>• When enabling <code>-dps</code>, set <code>fuelg -pcap</code> to the maximum power limit value for that range so the node receives the full benefit of dynamic power optimizer mode. When setting <code>fuelg -pcap</code> 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 <code>fuelg</code> command with no options to see the amount of power currently allocated.</li> <li>• When disabling <code>-dps</code>, make sure that the configured <code>fuelg -pcap</code> value for the node is not greater than the maximum power limit for the <code>-dps</code> disabled range. Reconfiguration of the <code>fuelg -pcap</code> value might be required to make sure that the power allocated for a node is not greater than the maximum power limit allowed.</li> </ul>	<p><code>fuelg -dps setting</code> where a <i>setting</i> of:</p> <ul style="list-style-type: none"> <li>• <code>off</code> (default) disables dynamic power optimizer for the compute node.</li> <li>• <code>on</code> enables dynamic power optimizer for the compute node.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Compute node:</p> <p><code>blade[x]</code> where <code>x</code> is the node bay number.</p>
<p><b>Favor performance over power - enable or disable for compute node</b></p>	<p>Turns the favor performance over power feature on or off for the specified compute node.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• A compute node must be turned on before you can enable the favor performance over power feature for it.</li> <li>• Not all compute nodes support the favor performance over power feature.</li> <li>• This feature can only be active if the dynamic power optimizer is enabled.</li> </ul>	<p><code>fuelg -fpop setting</code> where a <i>setting</i> of:</p> <ul style="list-style-type: none"> <li>• <code>off</code> (default) disables favor performance over power for the compute node.</li> <li>• <code>on</code> enables favor performance over power for the compute node.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Compute node:</p> <p><code>blade[x]</code> where <code>x</code> is the node bay number.</p>

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

To view Flex System Enterprise Chassis power trending information for the past 6 hours, while the Flex System Enterprise 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 Flex System Enterprise 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 Flex System Enterprise 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

Bay(s)	Module	Power State	Current	Allocated Power Max	Allocated Power 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 385 for a list of error messages that apply to all commands or "groups command errors" on page 415 for a list of error messages that are specific to the groups command.

Table 40. *groups* (Active Directory groups) command

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

Table 40. groups (Active Directory groups) command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<p><b>Add new Active Directory group</b></p>	<p>Adds a new Active Directory group.</p> <p><b>Notes:</b> When adding a new group you must specify:</p> <ul style="list-style-type: none"> <li>• a unique group name using the -n command option.</li> <li>• a role-based security level for the group using the -a command option.</li> </ul>	<p>groups - add -n <i>group_name</i> -a <i>group_authority</i> where:</p> <ul style="list-style-type: none"> <li>• <i>group_name</i> 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.</li> <li>• <i>group_authority</i> uses the following syntax: <ul style="list-style-type: none"> <li>- operator (Operator)</li> <li>-</li> <li>  <i>rb</i>s:<i>roles</i>:<i>scope</i></li> </ul>                     where the <i>roles</i> are one or more of the following authority levels, separated by a vertical bar (   ): <ul style="list-style-type: none"> <li>- super (Supervisor)</li> <li>- cam (Chassis User Account Management)</li> <li>- clm (Chassis Log Management)</li> <li>- co (Chassis Operator)</li> <li>- cc (Chassis Configuration)</li> <li>- ca (Chassis Administration)</li> <li>- bo (Blade Operator)</li> <li>- brp (Blade Remote Present)</li> <li>- bc (Blade Configuration)</li> <li>- ba (Blade Administration)</li> <li>- so (I/O Module Operator)</li> <li>- sc (I/O Module Configuration)</li> <li>- sa (I/O Module Administration)</li> </ul> </li> </ul> <p>(continued on next page)</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>
<p><b>Add new Active Directory group</b> (continued)</p>		<p>where the <i>scope</i> is one or more of the following devices, separated by a vertical bar (   ). Ranges of devices are separated by a dash ( - ).</p>	

Table 40. groups (Active Directory groups) command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
		<ul style="list-style-type: none"> <li>• <i>c n</i> (Chassis <i>n</i>, where <i>n</i> is 1 for the Active Directory environment.)</li> <li>• <i>b n</i> (Blade <i>n</i>, where <i>n</i> is a valid node bay number in the chassis)</li> <li>• <i>s n</i> (I/O module <i>n</i>, where <i>n</i> is a valid I/O-bay number in the chassis)</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	
<p><b>Set Active Directory group authority level</b></p>	<p>Sets the authority level for the specified Active Directory group.</p>	<p><code>groups -n <i>group_name</i> -a <i>group_authority</i></code>            where:</p> <ul style="list-style-type: none"> <li>• <i>group_name</i> is the unique alphanumeric string, up to 63 characters in length, that identifies the Active Directory group.</li> <li>• <i>group_authority</i> uses the following syntax:               <ul style="list-style-type: none"> <li>- <code>operator</code> (Operator)</li> <li>-</li> <li>- <code>rb:roles:scope</code>                    where the <i>roles</i> are one or more of the following authority levels, separated by a vertical bar ( ):                   <ul style="list-style-type: none"> <li>- <code>super</code> (Supervisor)</li> <li>- <code>cam</code> (Chassis User Account Management)</li> <li>- <code>clm</code> (Chassis Log Management)</li> <li>- <code>co</code> (Chassis Operator)</li> <li>- <code>cc</code> (Chassis Configuration)</li> <li>- <code>ca</code> (Chassis Administration)</li> <li>- <code>bo</code> (Blade Operator)</li> </ul> </li> </ul> </li> </ul>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where <i>x</i> is the primary CMM bay number.</p>

Table 40. groups (Active Directory groups) command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
		<ul style="list-style-type: none"> <li>- brp (Blade Remote Present)</li> <li>- bc (Blade Configuration)</li> <li>- ba (Blade Administration)</li> <li>- so (I/O Module Operator)</li> <li>- sc (I/O Module Configuration)</li> <li>- sa (I/O Module Administration)</li> </ul> <p>(continued on next page)</p>	
<p><b>Set Active Directory group authority level</b> (continued)</p>		<p>where the <i>scope</i> is one or more of the following devices, separated by a vertical bar ( ). Ranges of devices are separated by a dash (-).</p> <ul style="list-style-type: none"> <li>• <i>c n</i> (Chassis <i>n</i>, where <i>n</i> is 1 for the Active Directory environment.)</li> <li>• <i>b n</i> (Blade <i>n</i>, where <i>n</i> is a valid node bay number in the chassis)</li> <li>• <i>s n</i> (I/O module <i>n</i>, where <i>n</i> is a valid I/O-bay number in the chassis)</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	



Table 40. groups (Active Directory groups) command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Delete Active Directory group</b>	Delete the specified Active Directory group.	<pre>groups -n group_name -clear</pre> <p><i>group_name</i> is the unique alphanumeric string, up to 63 characters in length, that identifies the Active Directory group.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	Primary CMM:  <pre>mm[p]</pre> <pre>mm[P]</pre> <pre>mm[x]</pre> <p>where x is the primary CMM bay number.</p>

**Example:** To create an Active Directory group with a group name of admin1 that has supervisor rights to all Flex System components, while the Flex System Enterprise 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 Flex System Enterprise 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 Flex System Enterprise 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 Flex System Enterprise 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.



For the compute node 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 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.

For command targets other than a compute node, one of the following health states is returned. For the Flex System Enterprise Chassis, 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.

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

- Web interface: Critical , Attention , Normal 
- SNMP: Critical/Bad, Warning, Good
- CLI: Critical, Non-critical, 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 385 for a list of error messages that apply to all commands or “health command errors” on page 416 for a list of error messages that are specific to the health command.

Table 41. health command

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<p><b>Display health status</b></p>	<p>Displays the current health status of the command target.</p> <ul style="list-style-type: none"> <li>• Possible return values for the compute node target are: <ul style="list-style-type: none"> <li>– ok</li> <li>– non-critical</li> <li>– critical</li> </ul> </li> <li>• Possible return values for other targets are: <ul style="list-style-type: none"> <li>– ok</li> <li>– system level</li> <li>– non-critical</li> <li>– critical</li> </ul> </li> </ul>	<p>health</p>	<p>Flex System Enterprise Chassis:</p> <p>system</p> <p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p> <p>Compute node:</p> <p>blade[x] where x is the node bay number.</p> <p>I/O module:</p> <p>switch[x] where x is the I/O-bay number.</p> <p>Power supply:</p> <p>power[x] where x is the power supply bay number.</p> <p>Fan module:</p> <p>blower[x] where x is the fan module bay number.</p>
<p><b>Display health status for tree</b></p>	<p>Displays the current health status of the tree structure of devices present in the Flex System Enterprise Chassis, starting at the command target level. If CMM bays are part of the tree, they will be identified as primary or standby (redundant).</p> <ul style="list-style-type: none"> <li>• Possible return values for the compute node target are: <ul style="list-style-type: none"> <li>– ok</li> <li>– non-critical</li> <li>– critical</li> </ul> </li> <li>• Possible return values for other targets are: <ul style="list-style-type: none"> <li>– ok</li> <li>– system level</li> <li>– non-critical</li> <li>– critical</li> </ul> </li> </ul>	<p>health -l <i>depth</i> where <i>depth</i></p> <ul style="list-style-type: none"> <li>• 1 displays health status of the current command target</li> <li>• 2 , all , or a displays a full tree display, starting at the command target level</li> </ul>	<p>Flex System Enterprise Chassis:</p> <p>system</p> <p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p> <p>Compute node:</p> <p>blade[x] where x is the node bay number.</p>

Table 41. health command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
			<p>I/O module:</p> <p>switch[x] where x is the I/O-bay number.</p> <p>Power supply:</p> <p>power[x] where x is the power supply bay number.</p> <p>Fan module:</p> <p>blower[x] where x is the fan module bay number.</p>
<p><b>Display health status and alerts</b></p>	<p>Displays the current health status and active alerts for the command target.</p> <ul style="list-style-type: none"> <li>• Possible return values for the compute node target are: <ul style="list-style-type: none"> <li>– ok</li> <li>– non-critical</li> <li>– critical</li> </ul> </li> <li>• Possible return values for other targets are: <ul style="list-style-type: none"> <li>– ok</li> <li>– system level</li> <li>– non-critical</li> <li>– critical</li> </ul> </li> <li>• Active alert information provides short text descriptions of alerts that are active for each monitored component.</li> </ul> <p>The total amount of information returned from the <b>health -f</b> command is limited to 1024 bytes.</p>	<p>health -f</p>	<p>Flex System Enterprise Chassis:</p> <p>system</p> <p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p> <p>Compute node:</p> <p>blade[x] where x is the node bay number.</p> <p>I/O module:</p> <p>switch[x] where x is the I/O-bay number.</p> <p>Power supply:</p> <p>power[x] where x is the power supply bay number.</p> <p>Fan module:</p> <p>blower[x] where x is the fan module bay number.</p>

Table 41. health command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Display results with timestamp</b>	Adds display of timestamp information to status command output.	health -t <b>Note:</b> The -t option must be used with the -f option.	Flex System Enterprise Chassis: system  Primary CMM: mm[p] mm[P] mm[x] where x is the primary CMM bay number.  Compute node: blade[x] where x is the node bay number.  I/O module: switch[x] where x is the I/O-bay number.  Power supply: power[x] where x is the power supply bay number.  Fan module: 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 Flex System Enterprise Chassis, that are valid command targets, while the Flex System Enterprise 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
  bladegroup[3]
    blade[1] : OK
    blade[2] : Critical
    (04/04/13, 08:57:08) Node Node 03 - 02 message: System-management
    software, (IMM2 FW Failover) unsupported software version, node
    system-management processor firmware boot block.
  blade[4] : Non-Critical
  (04/04/13, 08:43:54) Node Node 04 device Storage back plane[01] VPD is
```

```

not valid.
blade[5] :           Critical
(04/04/13, 08:57:08) Node Node 05 message: System firmware, firmware
progress (Firmware Error) error. Error, See reference code BA15D001
(53087D2D BA15D001 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000)
bladeenclosure[7]
    blade[1] : OK
    blade[2] : OK
bladeenclosure[11]
    blade[1] : Critical
(04/04/13, 08:57:08) Node Node 11 - 01 message: System-management
software, (IMM2 FW Failover) unsupported software version, node
system-management processor firmware boot block.
    blade[2] : OK
blower[1] :         OK
blower[2] :         OK
blower[3] :         OK
blower[4] :         OK
blower[5] :         OK
blower[6] :         OK
blower[7] :         OK
blower[8] :         OK
blower[9] :         OK
blower[10]:        OK
power[1] :          Non-Critical
(04/04/13, 08:43:49) Power supply Power Supply 01 is off. AC fault.
    blower[1] : OK
power[2] :          Non-Critical
(04/04/13, 08:43:49) Power supply Power Supply 02 is off. AC fault.
    blower[1] : OK
power[3] :          Non-Critical
(04/04/13, 08:43:49) Power supply Power Supply 03 is off. AC fault.
    blower[1] : OK
power[4] :          OK
    blower[1] : OK
power[5] :          OK
    blower[1] : OK
power[6] :          OK
    blower[1] : OK
mm[2] :             OK
(04/04/13, 08:50:52) Hot air exiting from the rear of the chassis might
be recirculated in the inlet air at the front of the chassis. Slot 11:
28.00C, Slot 3: 21.00C.
switch[2] :         OK
switch[3] :         OK
mt[1] :            OK
fanmux[1] :         OK
fanmux[2] :         OK

```

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 385 for a list of error messages that apply to all commands or “help command errors” on page 417 for a list of error messages that are specific to the help command.

Table 42. 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 where <i>command</i> is any valid CLI root command (no options specified).	Any installed device.
		command -help where <i>command</i> is any valid CLI root command (no options specified).	Any installed device.
		command ? where <i>command</i> 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 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 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
    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 entries
    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 SQL 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 SQL status and view/edit SQL 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 385 for a list of error messages that apply to all commands or "history command errors" on page 417 for a list of error messages that are specific to the history command.

Table 43. *history command*

Function	What it does	Command	Target (see <i>paths in "Command targets" on page 6</i> )
<b>Command history</b>	Displays the last eight commands that were entered.	history	Any installed device.
<b>Re-enter previous command using numeric designation</b>	Re-enters a numerically-specified command from the command history.	!x 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 385 for a list of error messages that apply to all commands or “ifconfig command errors” on page 417 for a list of error messages that are specific to the ifconfig command.

Table 44. `ifconfig` command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Display primary CMM Ethernet channel 0 configuration</b></p>	<p>Displays the current configuration of Ethernet channel 0 for the primary CMM. Possible return values are:</p> <ul style="list-style-type: none"> <li>• enabled</li> <li>• disabled</li> <li>• <code>-i static_ip_address</code> (dotted decimal IPv4 IP address format)</li> <li>• <code>-g gateway_address</code> (dotted decimal IPv4 IP address format)</li> <li>• <code>-s subnet_mask</code> (dotted decimal IPv4 IP address format)</li> <li>• <code>-n hostname</code></li> <li>• <code>-c config_method</code></li> <li>• <code>-r data_rate</code></li> <li>• <code>-d duplex_mode</code></li> <li>• <code>-m mtu</code></li> <li>• <code>-l locally_administered_mac_addr</code></li> <li>• <code>-b burnedin_mac_address</code></li> <li>• <code>-dn domain_name</code></li> <li>• <code>-ipv6 ipv6_state</code></li> <li>• <code>-ipv6static static_ipv6_state</code></li> <li>• <code>-i6 static_ip_address</code> (IPv6 format)</li> <li>• <code>-p6 address_prefix_length</code></li> <li>• <code>-g6 gateway-default_route</code></li> <li>• <code>-dhcp6 dhcpv6_state</code></li> <li>• <code>-sa6 ipv6_stateless_autoconfig_state</code></li> </ul> <p>If IPv6 is enabled, the link-local address <code>link_local_address</code> (for IPv6 connection) also displays.</p> <p>If IPv6 and stateless auto-configuration (<code>-sa6</code>) are both enabled, the Stateless auto-config IP Addresses / Prefix Length <code>address_table</code> (table listing auto-generated IPv6 addresses and their prefix lengths) also displays.</p> <p>If there are two CMMs installed in the chassis and the <code>advfailover</code> command is set to <code>noswap</code>, the following items also display:</p> <ul style="list-style-type: none"> <li>• <code>-f floating_ip_address</code> (dotted decimal IPv4 IP address format)</li> <li>• <code>-f6 floating_ip_address</code> (IPv6 format)</li> </ul>	<p><code>ifconfig -eth0</code></p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where x is the primary CMM bay number.</p>
<p><b>Display standby CMM Ethernet channel 0 configuration</b></p>	<p>Displays the current configuration of Ethernet channel 0 for the standby CMM.</p> <p><b>Note:</b> If there are two CMMs installed in the chassis and the currently active <code>advfailover</code> setting</p>	<p><code>ifconfig -eth0 -o</code></p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code></p>

Table 44. *ifconfig* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
	<p>is off, there will be no current configuration of eth0 for the standby CMM.</p> <p>Possible return values are:</p> <ul style="list-style-type: none"> <li>• enabled</li> <li>• disabled</li> <li>• -i <i>static_ip_address</i> (dotted decimal IPv4 IP address format)</li> <li>• -g <i>gateway_address</i> (dotted decimal IPv4 IP address format)</li> <li>• -s <i>subnet_mask</i> (dotted decimal IPv4 IP address format)</li> <li>• -n <i>hostname</i></li> <li>• -c <i>config_method</i></li> <li>• -r <i>data_rate</i></li> <li>• -d <i>duplex_mode</i></li> <li>• -m <i>mtu</i></li> <li>• -l <i>locally_administered_mac_addr</i></li> <li>• -b <i>burnedin_mac_address</i></li> <li>• -dn <i>domain_name</i></li> <li>• -ipv6 <i>ipv6_state</i></li> <li>• -ipv6static <i>static_ipv6_state</i></li> <li>• -i6 <i>static_ip_address</i> (IPv6 format)</li> <li>• -p6 <i>address_prefix_length</i></li> <li>• -g6 <i>gateway-default_route</i></li> <li>• -dhcp6 <i>dhcpv6_state</i></li> <li>• -sa6 <i>ipv6_stateless_autoconfig_state</i></li> </ul> <p>If IPv6 is enabled, the link-local address <i>link_local_address</i> (for IPv6 connection) also displays.</p> <p>If IPv6 and stateless auto-configuration (-sa6) are both enabled, the Stateless auto-config IP Addresses / Prefix Length <i>address_table</i> (table listing auto-generated IPv6 addresses and their prefix lengths) also displays.</p>		<p>where x is the primary CMM bay number.</p> <p><b>Note:</b> Even though this command displays information for the standby CMM, it still must specify the primary CMM as the command target.</p>
<p><b>Set primary CMM Ethernet channel 0 static IP address (IPv4)</b></p>	<p>Sets the IPv4 static IP address for Ethernet channel 0 for the primary CMM.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• Static IPv4 parameters can not be set when the IPv4 configuration method is set to DHCP.</li> <li>• Changes made to the IPv4 configuration of the primary CMM take effect after the next reset of the primary CMM.</li> </ul>	<p><code>ifconfig -eth0 -i <i>ip_address</i></code>            where <i>ip_address</i> is the static IP address for Ethernet channel 0 in dotted decimal IP address format.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where x is the primary CMM bay number.</p>

Table 44. *ifconfig* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
	<ul style="list-style-type: none"> <li>• Including the <code>-apply</code> option when setting an IPv4 configuration option makes the change take effect immediately.</li> <li>• Use the <code>-apply</code> 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.</li> </ul>	<ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	
<b>Apply IPv4 configuration for primary CMM</b>	Places all outstanding IPv4 configuration made to the primary CMM into effect. <b>Note:</b> Using the <code>-apply</code> option places changes into effect without resetting the CMM.	<code>ifconfig -eth0 -apply</code> This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  <code>mm[p]</code> <code>mm[P]</code> <code>mm[x]</code> where <i>x</i> is the primary CMM bay number.
<b>Set primary CMM Ethernet channel 0 static IP address (IPv6)</b>	Sets the IPv6 static IP address for Ethernet channel 0 for the primary CMM.	<code>ifconfig -eth0 -i6 ip_address</code> where <i>ip_address</i> is the static IP address for Ethernet channel 0 in IPv6 format.  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  <code>mm[p]</code> <code>mm[P]</code> <code>mm[x]</code> where <i>x</i> is the primary CMM bay number.

Table 44. *ifconfig* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Set primary CMM Ethernet channel 0 floating IP address (IPv4)</b></p>	<p>Sets the IPv4 floating IP address for Ethernet channel 0 for the primary CMM.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• 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 <code>advfailover</code> command is set to <code>noswap</code>.</li> <li>• Changes made to the IPv4 configuration of the primary CMM take effect after the next reset of the primary CMM.</li> <li>• Including the <code>-apply</code> option when setting an IPv4 configuration option makes the change take effect immediately.</li> <li>• Use the <code>-apply</code> 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.</li> </ul>	<p><code>ifconfig -eth0 -f ip_ address</code>            where <i>ip_address</i> is the floating IP address for Ethernet channel 0 in dotted decimal IP address format.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where <i>x</i> is the primary CMM bay number.</p>
<p><b>Set primary CMM Ethernet channel 0 floating IP address (IPv6)</b></p>	<p>Sets the IPv6 floating IP address for Ethernet channel 0 for the primary CMM.</p> <p><b>Note:</b> 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 <code>advfailover</code> command is set to <code>noswap</code>.</p>	<p><code>ifconfig -eth0 -f6 ip_ address</code>            where <i>ip_address</i> is the floating IP address for Ethernet channel 0 in IPv6 format.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where <i>x</i> is the primary CMM bay number.</p>

Table 44. *ifconfig* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Set standby CMM Ethernet channel 0 static IP address (IPv4)</b></p>	<p>Sets the IPv4 static IP address for Ethernet channel 0 for the standby CMM.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• 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 <code>advfailover</code> command is set to <code>noswap</code>.</li> <li>• Static IPv4 parameters can not be set when the IPv4 configuration method is set to DHCP.</li> <li>• Changing the IPv4 static IP address for the standby CMM takes effect immediately.</li> </ul>	<p><code>ifconfig -eth0 -o -i ip_address</code>            where <i>ip_address</i> is the static IP address for Ethernet channel 0 in dotted decimal IP address format.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where <i>x</i> is the primary CMM bay number.</p> <p><b>Note:</b> Even though this command displays information for the standby CMM, it still must specify the primary CMM as the command target.</p>
<p><b>Set standby CMM Ethernet channel 0 static IP address (IPv6)</b></p>	<p>Sets the IPv6 static IP address for Ethernet channel 0 for the standby CMM.</p> <p><b>Note:</b> 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 <code>advfailover</code> command is set to <code>noswap</code>.</p>	<p><code>ifconfig -eth0 -o -i6 ip_address</code>            where <i>ip_address</i> is the static IP address for Ethernet channel 0 in IPv6 format.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where <i>x</i> is the primary CMM bay number.</p> <p><b>Note:</b> Even though this command displays information for the standby CMM, it still must specify the primary CMM as the command target.</p>

Table 44. *ifconfig* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Set primary CMM Ethernet channel 0 gateway IP address (IPv4)</b></p>	<p>Sets the IPv4 gateway IP address for Ethernet channel 0 for the primary CMM.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• Static IPv4 parameters can not be set when the IPv4 configuration method is set to DHCP.</li> <li>• Changes made to the IPv4 configuration of the primary CMM take effect after the next reset of the primary CMM.</li> <li>• Including the -apply option when setting an IPv4 configuration option makes the change take effect immediately.</li> <li>• 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.</li> </ul>	<p><code>ifconfig -eth0 -g <i>ip_address</i></code>            where <i>ip_address</i> is the gateway IP address for Ethernet channel 0 in dotted decimal IP address format.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>
<p><b>Set primary CMM Ethernet channel 0 gateway/default route (IPv6)</b></p>	<p>Sets the IPv6 gateway/default route for Ethernet channel 0 for the primary CMM.</p>	<p><code>ifconfig -eth0 -g6 <i>ip_address</i></code>            where <i>ip_address</i> is the gateway/default route for Ethernet channel 0 in IPv6 format.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>



Table 44. *ifconfig* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Set primary CMM Ethernet channel 0 subnet mask (IPv4)</b></p>	<p>Sets the IPv4 subnet mask for Ethernet channel 0 for the primary CMM.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• Static IPv4 parameters can not be set when the IPv4 configuration method is set to DHCP.</li> <li>• Changes made to the IPv4 configuration of the primary CMM take effect after the next reset of the primary CMM.</li> <li>• Including the <code>-apply</code> option when setting an IPv4 configuration option makes the change take effect immediately.</li> <li>• Use the <code>-apply</code> 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.</li> </ul>	<p><code>ifconfig -eth0 -s <i>sub_mask</i></code>            where <i>sub_mask</i> is the subnet mask for Ethernet channel 0 in dotted decimal IP address format.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where <i>x</i> is the primary CMM bay number.</p>
<p><b>Set primary CMM Ethernet channel 0 hostname</b></p>	<p>Sets the host name for Ethernet channel 0 for the primary CMM.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• Changes made to the IPv4 configuration of the primary CMM take effect after the next reset of the primary CMM.</li> <li>• Including the <code>-apply</code> option when setting an IPv4 configuration option makes the change take effect immediately.</li> <li>• Use the <code>-apply</code> 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.</li> </ul>	<p><code>ifconfig -eth0 -n <i>hostname</i></code>            where <i>hostname</i> 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.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where <i>x</i> is the primary CMM bay number.</p>

Table 44. *ifconfig* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Set standby CMM Ethernet channel 0 hostname</b></p>	<p>Sets the host name for Ethernet channel 0 for the standby CMM.</p> <p><b>Note:</b> Changes made to the host name of the standby CMM take effect immediately.</p>	<p><code>ifconfig -eth0 -o -n hostname</code>            where <i>hostname</i> 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.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p> <p><b>Note:</b> Even though this command displays information for the standby CMM, it still must specify the primary CMM as the command target.</p>
<p><b>Set primary CMM Ethernet channel 0 IPv4 configuration method</b></p>	<p>Sets the IPv4 configuration method for Ethernet channel 0 for the primary CMM.</p> <p>A value of <code>dhens</code> will try the DHCP configuration and default to the static IP configuration if DHCP is unsuccessful after 2 minutes.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Static IPv4 parameters can not be set when the IPv4 configuration method is set to DHCP.</li> <li>• Changes made to the IPv4 configuration of the primary CMM take effect after the next reset of the primary CMM.</li> <li>• Including the <code>-apply</code> option when setting an IPv4 configuration option makes the change take effect immediately.</li> <li>• Use the <code>-apply</code> option by itself after setting multiple IPv4 configuration options for an Ethernet channel to make all</li> </ul>	<p><code>ifconfig -eth0 -c config_method</code>            where <i>config_method</i> is</p> <ul style="list-style-type: none"> <li>• dhcp</li> <li>• static</li> <li>• dhens</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>

Table 44. *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.		
<b>Set primary CMM Ethernet channel 0 data rate</b>	Sets the data rate for Ethernet channel 0 for the primary CMM. <b>Note:</b> Changes made to the data rate of the primary CMM take effect after the next reset of the primary CMM.	<p><code>ifconfig -eth0 -r <i>data_rate</i></code>            where <i>data_rate</i> is</p> <ul style="list-style-type: none"> <li>• 10</li> <li>• 100</li> <li>• auto</li> <li>• 1000auto</li> </ul> <p><b>Note:</b> When set to 1000auto, the duplex mode is automatically changed to full.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Set primary CMM Ethernet channel 0 duplex mode</b>	Sets the duplex mode for Ethernet channel 0 for the primary CMM. <b>Note:</b> Changes made to the duplex mode of the primary CMM take effect after the next reset of the primary CMM.	<p><code>ifconfig -eth0 -d <i>duplex_mode</i></code>            where <i>duplex_mode</i> is</p> <ul style="list-style-type: none"> <li>• auto</li> <li>• half</li> <li>• full</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 44. *ifconfig* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Set CMM Ethernet channel 0 MTU</b>	Sets the MTU (maximum transmission unit) for Ethernet channel 0 for the CMM.	<pre>ifconfig -eth0 -m <i>mtu</i></pre> where <i>mtu</i> is between 60 and 1500, inclusive.  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  <pre>mm[p]</pre> <pre>mm[P]</pre> <pre>mm[x]</pre> where <i>x</i> is the primary CMM bay number.
<b>Set primary CMM Ethernet channel 0 static MAC address (locally administered)</b>	Sets the locally administered MAC address to the specified MAC address for Ethernet channel 0 for the primary CMM.  <b>Note:</b> Changes made to the IP configuration of the primary CMM take effect after the next reset of the primary CMM.	<pre>ifconfig -eth0 -l <i>address</i></pre> where <i>address</i> 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).  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  <pre>mm[p]</pre> <pre>mm[P]</pre> <pre>mm[x]</pre> where <i>x</i> is the primary CMM bay number.

Table 44. *ifconfig* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Set standby CMM Ethernet channel 0 static MAC address (locally administered)</b></p>	<p>Sets the locally administered MAC address to the specified MAC address for Ethernet channel 0 for the standby CMM.  <b>Note:</b> Changes made to the locally administered MAC address of the standby CMM take effect immediately.</p>	<p><code>ifconfig -eth0 -o -l address</code>            where <i>address</i> 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).</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where <i>x</i> is the primary CMM bay number.</p> <p><b>Note:</b> Even though this command displays information for the standby CMM, it still must specify the primary CMM as the command target.</p>
<p><b>Set primary CMM Ethernet channel 0 domain name</b></p>	<p>Sets the domain name for Ethernet channel 0 for the primary CMM.  <b>Note:</b> Changes made to the IP configuration of the primary CMM take effect after the next reset of the primary CMM.</p>	<p><code>ifconfig -eth0 -dn domain</code>            where <i>domain</i> is an alphanumeric string up to 127 characters in length. The domain name must contain at least one dot (.).</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where <i>x</i> is the primary CMM bay number.</p>

Table 44. *ifconfig* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Set standby CMM Ethernet channel 0 domain name</b>	Sets the domain name for Ethernet channel 0 for the standby CMM.	<p><code>ifconfig -o -eth0 -dn <i>domain</i></code>            where <i>domain</i> is an alphanumeric string up to 127 characters in length. The domain name must contain at least one dot (.).</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  <code>mm[p]</code> <code>mm[P]</code> <code>mm[x]</code> where <i>x</i> is the primary CMM bay number.
<b>Enable / disable static IPv6 configuration for CMM Ethernet channel 0</b>	Enable or disable static IPv6 configuration for Ethernet channel 0 for the CMM.	<p><code>ifconfig -eth0 -ipv6static <i>state</i></code>            where <i>state</i> is enabled or disabled .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  <code>mm[p]</code> <code>mm[P]</code> <code>mm[x]</code> where <i>x</i> is the primary CMM bay number.
<b>Set CMM Ethernet channel 0 address prefix length</b>	Sets the IPv6 address prefix length for Ethernet channel 0 for the CMM.	<p><code>ifconfig -eth0 -p6 <i>length</i></code>            where <i>length</i> is between 0 and 128 (inclusive).</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  <code>mm[p]</code> <code>mm[P]</code> <code>mm[x]</code> where <i>x</i> is the primary CMM bay number.

Table 44. *ifconfig* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Enable / disable DHCPv6 for CMM Ethernet channel 0</b>	Enable or disable static DHCPv6 for Ethernet channel 0 for the CMM.	<p><code>ifconfig -eth0 -dhcp6 state</code>            where <i>state</i> is enabled or disabled .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where <i>x</i> is the primary CMM bay number.</p>
<b>Enable / disable IPv6 stateless auto-configuration for CMM for Ethernet channel 0</b>	Enable or disable IPv6 stateless auto-configuration for Ethernet channel 0 for the CMM.	<p><code>ifconfig -eth0 -sa6 state</code>            where <i>state</i> is enabled or disabled .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where <i>x</i> is the primary CMM bay number.</p>
<b>Display network configuration status for compute node</b>	Displays the network interfaces and network status for the specified compute node.	<code>ifconfig</code>	<p>Compute node:</p> <p><code>blade[x]</code>            where <i>x</i> is the node bay number.</p>
<b>Display configuration information for network interface</b>	Displays the network interface type and number (such as <code>-eth0</code> ), network interface state (up or down), and other network interface configuration information for the specified network interface in the specified compute node.	<p><code>ifconfig -interface_label</code>            where <i>interface_label</i> is any interface label reported by the compute node that specifies both the interface type and channel number. For example, <code>eth0</code> for Ethernet channel 0. Valid interface types include:</p> <ul style="list-style-type: none"> <li>• <code>usb</code> for USB</li> <li>• <code>eth</code> for Ethernet</li> </ul> <p>Valid interface types for a specific compute node can be seen by running the <code>ifconfig</code> command with no interface argument.</p>	<p>Compute node:</p> <p><code>blade[x]</code>            where <i>x</i> is the node bay number.</p>

Table 44. *ifconfig* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Set compute node network interface static IP address (IPv4)</b></p>	<p>Sets the IPv4 static IP address for the specified network interface of the specified compute node.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• This command will run only if the target compute node supports manual configuration of its management network interface.</li> <li>• Static IPv4 parameters can not be set when the IPv4 configuration method is set to DHCP.</li> </ul>	<p><code>ifconfig -interface_label -i ip_address</code>            where:</p> <ul style="list-style-type: none"> <li>• <i>interface_label</i> 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:               <ul style="list-style-type: none"> <li>– usb for USB</li> <li>– eth for Ethernet</li> </ul> </li> <li>• <i>ip_address</i> is the static IP address for network interface in dotted decimal IP address format.</li> </ul> <p>Valid interface types for a specific compute node can be seen by running the <code>ifconfig</code> command with no interface argument.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Compute node:</p> <p>blade[x]            where x is the node bay number.</p>
<p><b>Set compute node network interface static IP address (IPv6)</b></p>	<p>Sets the IPv6 static IP address for the specified network interface of the specified compute node.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• This command will run only if the target compute node supports manual IPv6 configuration of its management network interface.</li> <li>• A static IPv6 configuration ID is required for network interfaces that support more than one static configuration.</li> </ul>	<p><code>ifconfig -interface_label -i6 ip_address -id id</code>            where:</p> <ul style="list-style-type: none"> <li>• <i>interface_label</i> 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:               <ul style="list-style-type: none"> <li>– usb for USB</li> <li>– eth for Ethernet</li> </ul> </li> <li>• <i>ip_address</i> is the static IP address for Ethernet</li> </ul>	<p>Compute node:</p> <p>blade[x]            where x is the node bay number.</p>



Table 44. *ifconfig* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
		<p>channel <i>x</i> in IPv6 format.</p> <ul style="list-style-type: none"> <li>• <i>id</i> is the static IPv6 configuration ID.</li> </ul> <p>Valid interface types for a specific compute node can be seen by running the <code>ifconfig</code> command with no interface argument.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	
<p><b>Set compute node network interface gateway IP address (IPv4)</b></p>	<p>Sets the IPv4 gateway IP address for the specified network interface of the specified compute node.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• This command will run only if the target compute node supports manual configuration of its management network interface.</li> <li>• Static IPv4 parameters can not be set when the IPv4 configuration method is set to DHCP.</li> </ul>	<p><code>ifconfig -interface_label -g ip_address</code> where:</p> <ul style="list-style-type: none"> <li>• <i>interface_label</i> is any interface label reported by the compute node that specifies both the interface type and channel number. For example, <code>eth0</code> for Ethernet channel 0. Valid interface types include: <ul style="list-style-type: none"> <li>– <code>usb</code> for USB</li> <li>– <code>eth</code> for Ethernet</li> </ul> </li> <li>• <i>ip_address</i> is the gateway IP address for Ethernet channel <i>x</i> in dotted decimal IP address format.</li> </ul> <p>Valid interface types for a specific compute node can be seen by running the <code>ifconfig</code> command with no interface argument.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p>	<p>Compute node:</p> <p><code>blade[x]</code> where <i>x</i> is the node bay number.</p>

Table 44. *ifconfig* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
		<ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	
<b>Set compute node network interface gateway/default route (IPv6)</b>	Sets the IPv6 gateway/default route for the specified network interface of the specified compute node. <b>Notes:</b> <ul style="list-style-type: none"> <li>• This command will run only if the target compute node supports manual IPv6 configuration of its management network interface..</li> <li>• A static IPv6 configuration ID is required for network interfaces that support more than one static configuration.</li> </ul>	<pre>ifconfig -interface_label -g6 ip_address -id id</pre> where: <ul style="list-style-type: none"> <li>• <i>interface_label</i> is any interface label reported by the compute node that specifies both the interface type and channel number. For example, <code>eth0</code> for Ethernet channel 0. Valid interface types include:               <ul style="list-style-type: none"> <li>– <code>usb</code> for USB</li> <li>– <code>eth</code> for Ethernet</li> </ul> </li> <li>• <i>ip_address</i> is the gateway/default route for Ethernet channel <i>x</i> in IPv6 format.</li> <li>• <i>id</i> is the static IPv6 configuration ID.</li> </ul> <p>Valid interface types for a specific compute node can be seen by running the <code>ifconfig</code> command with no interface argument.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Compute node:  <code>blade[x]</code> where <i>x</i> is the node bay number.

Table 44. *ifconfig* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Set compute node network interface subnet mask (IPv4)</b></p>	<p>Sets the IPv4 subnet mask for the specified network interface of the specified compute node.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This command will run only if the target compute node supports manual configuration of its management network interface.</li> <li>Static IPv4 parameters can not be set when the IPv4 configuration method is set to DHCP.</li> </ul>	<p><code>ifconfig -interface_label -s sub_mask</code>            where:</p> <ul style="list-style-type: none"> <li><i>interface_label</i> is any interface label reported by the compute node that specifies both the interface type and channel number. For example, <code>eth0</code> for Ethernet channel 0. Valid interface types include:               <ul style="list-style-type: none"> <li><code>usb</code> for USB</li> <li><code>eth</code> for Ethernet</li> </ul> </li> <li><i>sub_mask</i> is the subnet mask for Ethernet channel <i>x</i> in dotted decimal IP address format.</li> </ul> <p>Valid interface types for a specific compute node can be seen by running the <code>ifconfig</code> command with no interface argument.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Blade configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Compute node:</p> <p><code>blade[x]</code>            where <i>x</i> is the node bay number.</p>
<p><b>Set compute node network interface IPv4 configuration method</b></p>	<p>Sets the IPv4 configuration method for the specified network interface of the specified compute node. A value of <code>dhcens</code> will try the DHCP configuration and default to the static IP configuration if DHCP is unsuccessful after 2 minutes.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This command will run only if the target compute node supports manual configuration of its management network interface.</li> <li>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</li> </ul>	<p><code>ifconfig -interface_label -c config_method</code>            where:</p> <ul style="list-style-type: none"> <li><i>interface_label</i> is any interface label reported by the compute node that specifies both the interface type and channel number. For example, <code>eth0</code> for Ethernet channel 0. Valid interface types include:               <ul style="list-style-type: none"> <li><code>usb</code> for USB</li> <li><code>eth</code> for Ethernet</li> </ul> </li> <li><i>config_method</i> is               <ul style="list-style-type: none"> <li><code>dhcp</code></li> </ul> </li> </ul>	<p>Compute node:</p> <p><code>blade[x]</code>            where <i>x</i> is the node bay number.</p>

Table 44. *ifconfig* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
	<p>during start up. When this occurs, the IP address might not be reachable if multiple devices were started with the same static IP address.</p> <ul style="list-style-type: none"> <li>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 Flex System Manager hardware, if it is installed).</li> <li>Static IPv4 parameters can not be set when the IPv4 configuration method is set to DHCP.</li> </ul>	<ul style="list-style-type: none"> <li><code>static</code></li> <li><code>dthens</code></li> </ul> <p>Valid interface types for a specific compute node can be seen by running the <code>ifconfig</code> command with no interface argument.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Blade configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	
<p><b>Enable / disable IPv4 addressing for compute node</b></p>	<p>Enable or disable IPv4 addressing for the specified network interface of the specified compute node.</p>	<p><code>ifconfig -interface_label -ipv4 state</code> where:</p> <ul style="list-style-type: none"> <li><code>interface_label</code> is any interface label reported by the compute node that specifies both the interface type and channel number. For example, <code>eth0</code> for Ethernet channel 0. Valid interface types include: <ul style="list-style-type: none"> <li><code>usb</code> for USB</li> <li><code>eth</code> for Ethernet</li> </ul> </li> <li><code>state</code> is enabled or disabled .</li> </ul> <p>Valid interface types for a specific compute node can be seen by running the <code>ifconfig</code> command with no interface argument.</p>	<p>Compute node:</p> <p><code>blade[x]</code> where <code>x</code> is the node bay number.</p>

Table 44. `ifconfig` command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
		<p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	
<p><b>Set compute node address prefix length</b></p>	<p>Sets the IPv6 address prefix length for the specified network interface of the specified compute node.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• This command will run only if the target compute node supports manual IPv6 configuration of its management network interface.</li> <li>• A static IPv6 configuration ID is required for network interfaces that support more than one static configuration.</li> </ul>	<p><code>ifconfig -interface_label -p6 length -id id</code>            where:</p> <ul style="list-style-type: none"> <li>• <code>interface_label</code> is any interface label reported by the compute node that specifies both the interface type and channel number. For example, <code>eth0</code> for Ethernet channel 0. Valid interface types include:               <ul style="list-style-type: none"> <li>– <code>usb</code> for USB</li> <li>– <code>eth</code> for Ethernet</li> </ul> </li> <li>• <code>length</code> is between 0 and 128 (inclusive).</li> <li>• <code>id</code> is the static IPv6 configuration ID.</li> </ul> <p>Valid interface types for a specific compute node can be seen by running the <code>ifconfig</code> command with no interface argument.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Compute node:</p> <p><code>blade[x]</code>            where <code>x</code> is the node bay number.</p>

Table 44. *ifconfig* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Enable / disable DHCPv6 for compute node</b></p>	<p>Enable or disable static DHCPv6 for the specified network interface of the specified compute node.</p> <p><b>Note:</b> This command will run only if the target compute node supports manual IPv6 configuration of its management network interface.</p>	<p><code>ifconfig -interface_label -dhcp6 state</code>            where:</p> <ul style="list-style-type: none"> <li>• <i>interface_label</i> 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:               <ul style="list-style-type: none"> <li>– usb for USB</li> <li>– eth for Ethernet</li> </ul> </li> <li>• <i>state</i> is enabled or disabled .</li> </ul> <p>Valid interface types for a specific compute node can be seen by running the <code>ifconfig</code> command with no interface argument.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Compute node:</p> <p>blade[x]            where x is the node bay number.</p>
<p><b>Enable / disable IPv6 stateless auto-configuration for compute node</b></p>	<p>Enable or disable IPv6 stateless auto-configuration for the specified network interface of the specified compute node.</p> <p><b>Note:</b> This command will run only if the target compute node supports manual IPv6 configuration of its management network interface.</p>	<p><code>ifconfig -interface_label -sa6 state</code>            where:</p> <ul style="list-style-type: none"> <li>• <i>interface_label</i> 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:               <ul style="list-style-type: none"> <li>– usb for USB</li> <li>– eth for Ethernet</li> </ul> </li> <li>• <i>state</i> is enabled or disabled</li> </ul> <p>Valid interface types for a specific compute node</p>	<p>Compute node:</p> <p>blade[x]            where x is the node bay number.</p>

Table 44. *ifconfig* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
		<p>can be seen by running the <i>ifconfig</i> command with no interface argument.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	
<p><b>Display network settings for I/O module</b></p>	<p>Displays network settings for the specified I/O module. Valid return values are:</p> <ul style="list-style-type: none"> <li>• I/O-module type</li> <li>• -i <i>ip_address</i> (dotted decimal IPv4 IP address format)</li> <li>• -s <i>subnet_mask</i> (dotted decimal IPv4 IP address format)</li> <li>• -g <i>gateway_address</i> (dotted decimal IPv4 IP address format)</li> <li>• -em <i>ext_mgt_status</i></li> <li>• -ep <i>ext_port_status</i></li> <li>• -pm <i>enabled/disabled</i> (protected mode)</li> <li>• -pip <i>enabled/disabled</i></li> <li>• -c <i>config_method</i></li> <li>• -ipv6 <i>ipv6_state</i></li> <li>• -ipv6static <i>static_ipv6_state</i></li> <li>• -i6 <i>static_ip_address</i> (IPv6 format)</li> <li>• -p6 <i>address_prefix_length</i> (IPv6 format)</li> <li>• -g6 <i>gateway-default_route</i> (IPv6 format)</li> <li>• -dhcp6 <i>dhcpv6_state</i></li> <li>• -sa6 <i>ipv6_stateless_autoconfig_state</i></li> </ul> <p>If IPv6 is enabled, the link-local address <i>link_local_address</i> (for IPv6 connection) also displays.</p> <p>If IPv6 and stateless auto-configuration (-sa6) are both enabled, the Stateless auto-config IP Addresses / Prefix Length <i>address_table</i> (table listing auto-generated IPv6 addresses and their prefix lengths) also displays.</p>	<p><i>ifconfig</i></p>	<p>I/O module:</p> <p><i>switch[x]</i> where <i>x</i> is the I/O-bay number.</p>

Table 44. *ifconfig* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Set I/O module IPv4 network configuration method</b></p>	<p>Sets the IPv4 network configuration method for the specified I/O module.</p> <p>A value of <code>dhcens</code> will try the DHCP configuration and default to the static IP configuration if DHCP is unsuccessful after 2 minutes.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• This command will run only if the target I/O module supports manual configuration of its management network interface.</li> <li>• 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.</li> <li>• Static IPv4 parameters can not be set when the IPv4 configuration method is set to DHCP.</li> </ul>	<p><code>ifconfig -c config_method</code>            where <i>config_method</i> is</p> <ul style="list-style-type: none"> <li>• <code>dhcp</code></li> <li>• <code>static</code></li> <li>• <code>dhcens</code></li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• I/O module configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>I/O module:</p> <p><code>switch[x]</code>            where <i>x</i> is the I/O-bay number.</p>
<p><b>Set starting IP address for I/O module (IPv4)</b></p>	<p>Sets the IPv4 IP addresses for the specified I/O module.</p> <p><b>Note:</b> Static IPv4 parameters can not be set when the IPv4 configuration method is set to DHCP.</p>	<p><code>ifconfig -i ip_address</code>            where <i>ip_address</i> is the IP address of the specified I/O module in dotted decimal IP address format.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• I/O module configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>I/O module:</p> <p><code>switch[x]</code>            where <i>x</i> is the I/O-bay number.</p>



Table 44. *ifconfig* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Set starting IP address for I/O module (IPv6)</b>	Sets the IPv6 static IP address for the specified I/O module.	<p><code>ifconfig -i6 ip_address</code>            where <i>ip_address</i> is the static IP address for the specified I/O module in IPv6 format.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• I/O module configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	I/O module:  switch[x] where x is the I/O-bay number.
<b>Set I/O-module gateway IP address (IPv4)</b>	Sets the gateway IPv4 IP address for the specified I/O module. <b>Note:</b> Static IPv4 parameters can not be set when the IPv4 configuration method is set to DHCP.	<p><code>ifconfig -g ip_address</code>            where <i>ip_address</i> is the gateway IP address for the I/O module in dotted decimal IP address format.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• I/O module configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	I/O module:  switch[x] where x is the I/O-bay number.
<b>Set I/O-module gateway IP address (IPv6)</b>	Sets the IPv6 gateway/default route for the specified I/O module.	<p><code>ifconfig -g6 ip_address</code>            where <i>ip_address</i> is the gateway IP address for the I/O module in IPv6 format.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• I/O module configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	I/O module:  switch[x] where x is the I/O-bay number.

Table 44. *ifconfig* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Keep new IP address configuration for I/O-module after reset</b></p>	<p>Retains a new IP address configuration after the specified I/O module is reset.  <b>Note:</b> 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.</p>	<p><code>ifconfig -pip enabled</code>            This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• I/O module administration</li> <li>• I/O module configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>I/O module:   <code>switch[x]</code>            where <i>x</i> is the I/O-bay number.</p>
<p><b>Revert to old IP address configuration for I/O-module after reset</b></p>	<p>Reverts IP address to old configuration after the specified I/O module is reset.  <b>Note:</b> 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.</p>	<p><code>ifconfig -pip disabled</code>            This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• I/O module administration</li> <li>• I/O module configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>I/O module:   <code>switch[x]</code>            where <i>x</i> is the I/O-bay number.</p>
<p><b>Set I/O-module subnet mask (IPv4)</b></p>	<p>Sets the IPv4 subnet mask for the specified I/O module.  <b>Note:</b> Static IPv4 parameters can not be set when the IPv4 configuration method is set to DHCP.</p>	<p><code>ifconfig -s <i>sub_mask</i></code>            where <i>sub_mask</i> is the subnet mask for the I/O module in dotted decimal IP address format.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• I/O module configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>I/O module:   <code>switch[x]</code>            where <i>x</i> is the I/O-bay number.</p>

Table 44. *ifconfig* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Enable / disable external management for I/O module</b>	Enables or disables external management on all ports for the specified I/O module.	<p><code>ifconfig -em state</code>            where <i>state</i> is enabled or disabled .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• I/O module configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	I/O module:  <code>switch[x]</code> where <i>x</i> is the I/O-bay number.
<b>Enable Ethernet interface for I/O module</b>	Enables the Ethernet interface for the specified I/O module.	<p><code>ifconfig -up</code>            This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• I/O module configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	I/O module:  <code>switch[x]</code> where <i>x</i> is the I/O-bay number.
<b>Disable Ethernet interface for I/O module</b>	Disables the Ethernet interface for the specified I/O module.	<p><code>ifconfig -down</code>            This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• I/O module configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	I/O module:  <code>switch[x]</code> where <i>x</i> is the I/O-bay number.
<b>Enable / disable external ports for I/O module</b>	Enables or disables external ports for the specified I/O module.	<p><code>ifconfig -ep state</code>            where <i>state</i> is enabled or disabled .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• I/O module configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	I/O module:  <code>switch[x]</code> where <i>x</i> is the I/O-bay number.

Table 44. *ifconfig* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Enable / disable protected mode for I/O module</b>	Enables or disables protected mode for the specified I/O module.	<p><code>ifconfig -pm state</code>            where <i>state</i> is enabled or disabled .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• I/O module configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>I/O module:</p> <p><code>switch[x]</code>            where <i>x</i> is the I/O-bay number.</p>
<b>Enable / disable static IPv6 configuration for I/O module</b>	Enable or disable static IPv6 configuration for the specified I/O module.	<p><code>ifconfig -ipv6static state</code>            where <i>state</i> is enabled or disabled .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• I/O module configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>I/O module:</p> <p><code>switch[x]</code>            where <i>x</i> is the I/O-bay number.</p>
<b>Set I/O module address prefix length</b>	Sets the IPv6 address prefix length for the specified I/O module.	<p><code>ifconfig -p6 length</code>            where <i>length</i> is between 0 and 128 (inclusive).</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• I/O module configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>I/O module:</p> <p><code>switch[x]</code>            where <i>x</i> is the I/O-bay number.</p>

Table 44. *ifconfig* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Enable / disable DHCPv6 for I/O module</b>	Enable or disable static DHCPv6 for the specified I/O module.	<code>ifconfig -dhcp6 state</code> where <i>state</i> is enabled or disabled .  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• I/O module configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	I/O module:  <code>switch[x]</code> where <i>x</i> is the I/O-bay number.
<b>Enable / disable IPv6 stateless auto-configuration for I/O module</b>	Enable or disable IPv6 stateless auto-configuration for the specified I/O module.	<code>ifconfig -sa6 state</code> where <i>state</i> is enabled or disabled .  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• I/O module configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	I/O module:  <code>switch[x]</code> where <i>x</i> 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 Flex System Enterprise 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 Flex System Enterprise 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 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 385 for a list of error messages that apply to all commands or “info command errors” on page 421 for a list of error messages that are specific to the info command.

Table 45. info command

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<p><b>Display component information</b></p>	<p>Displays identification and configuration information for the command target.</p>	<p>info  <b>Note:</b> Only one target at a time can be viewed with the info command.</p>	<p>Flex System Enterprise Chassis:              system</p> <p>Primary or standby CMM:              mm[p]              mm[P]              mm[s]              mm[S]              mm[x]              where x is the primary or standby CMM bay number.</p> <p>Compute node:              blade[x]              where x is the node bay number.</p> <p>Fan logic module:              fanmux[x]              where x is the fan logic module bay number.</p> <p>Fan module:              blower[x]              where x is the fan module bay number.</p> <p>Compute node expansion adapter:              exp[x]              where x is the expansion adapter number.</p> <p>Compute node management card:              mgmtcrd[x]              where x is the management card number.</p> <p>Compute node system-management processor:              sp</p> <p><i>(continued on next page)</i></p>

Table 45. info command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<p><b>Display component information</b> (continued)</p>			<p>Compute node expansion node:  <code>be[x]</code>                      where <i>x</i> is the expansion node number.</p> <p>Compute node microprocessor:  <code>cpu[x]</code>                      where <i>x</i> is the microprocessor number.</p> <p>Compute node memory:  <code>memory[x]</code>                      where <i>x</i> is the memory module number.</p> <p>Compute node flash DIMM storage module:  <code>flashdim[x]</code>                      where <i>x</i> identifies the flash DIMM storage module number.</p> <p>Compute node add-in card:  <code>addin[x]</code>                      where <i>x</i> is the add-in card number.</p> <p>Compute node alarm panel:  <code>tap[x]</code>                      where <i>x</i> is the alarm panel number.</p> <p>Storage backplane:  <code>stgbkplane[x]</code>                      where <i>x</i> is the storage backplane number.</p> <p>Storage expansion enclosure:  <code>bladeenclosure[x]</code>                      where <i>x</i> is the storage expansion enclosure number.</p>



Table 45. info command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
			I/O module: switch[x] where x is the I/O-bay number.  (continued on next page)
<b>Display component information</b> (continued)			Power supply: power[x] where x is the power supply bay number.  Rear LED card: mt[x] where x is the rear LED card.
<b>Display management channel path information</b>	Displays the management channel path information for the specified command target. The following information is returned: <ul style="list-style-type: none"> <li>• Channel status</li> <li>• MAC address</li> </ul> <b>Note:</b> 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: blade[x] where x is the node bay number.  I/O module: switch[x] 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 Flex System Enterprise 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: IBM (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: IBM Flex Midplane
Global ID: 9TY48MBX
```

```
system> info -T blade[6]
Name: Node 05 ( node5 )
UUID: 60C2 2B17 0C5C B060 C183 060C DB30 6108
Manufacturer: IBM (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: 11/20/2012  
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: IBM (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: 1A0033N  
Rel date: 09/14/2012  
Rev: 1.80  
Role: Primary

MP

Build ID: 1A0033N  
Rel date: 09/14/2012  
Rev: 1.80  
Role: Backup

UEFI

Build ID: CCE111NUS  
Rel date: 03/16/2012  
Rev: 1.00  
Role: Primary

UEFI

Build ID: CCE111NUS  
Rel date: 03/16/2012  
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: IBM (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: IBM 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 385 for a list of error messages that apply to all commands or “iocomp command errors” on page 422 for a list of error messages that are specific to the iocomp command.

Table 46. *iocomp* command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display compatibility between all compute nodes and I/O modules</b>	Displays I/O module compatibility information for all compute nodes and I/O modules.	<code>iocomp</code>	Flex System Enterprise Chassis: system
<b>Display compute node compatibility details</b>	Displays detailed I/O module compatibility information for the specified compute node.	<code>iocomp</code>	Compute node: blade[x] where x is the node bay number.
<b>Display I/O module compatibility details</b>	Displays detailed compatibility information for the specified I/O module.	<code>iocomp</code>	I/O module: switch[x] 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 317 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 385 for a list of error messages that apply to all commands or “`ldapcfg` command errors” on page 422 for a list of error messages that are specific to the `ldapcfg` command.

Table 47. *ldapcfg* command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display LDAP settings</b>	Displays the LDAP settings for the CMM.	ldapcfg	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Set LDAP security version</b>	Sets version of LDAP security used by the CMM. <b>Notes:</b> <ul style="list-style-type: none"> <li>• If the version is set to v1, the following values must also be set: <ul style="list-style-type: none"> <li>– A group filter using the <b>-gf</b> command option.</li> <li>– A group search attribute using the <b>-gsa</b> command option.</li> <li>– A login permission attribute using the <b>-lpa</b> command option.</li> </ul> </li> <li>• If the version is set to v2, the LDAP name must also be set using the <b>-t</b> command option.</li> </ul>	ldapcfg -v <i>version</i> where <i>version</i> is: <ul style="list-style-type: none"> <li>• v1 for old user permission model</li> <li>• v2 for the enhanced role-based security model</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.



Table 47. `ldapcfg` command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<p><b>Set LDAP group filter</b></p>	<p>Sets the group filter for the CMM that can be used for authentication during LDAP server login.</p> <p><b>Note:</b> For a group filter to be used, LDAP security must be set to v1 using the <code>-v</code> command option.</p>	<p><code>ldapcfg -gf "filter"</code>            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.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>
<p><b>Set LDAP group search attribute</b></p>	<p>Sets the group search attribute that represents groups of user IDs stored on the LDAP server. On Active Directory servers, the group search attribute is typically set to "memberOf". On eDirectory servers, it is typically set to "groupMembership".</p> <p>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".</p> <p><b>Note:</b> For a group search attribute to be used, LDAP security must be set to v1 using the <code>-v</code> command option.</p>	<p><code>ldapcfg -gsa "GSA"</code>            where "GSA" is a quote-delimited string of up to 23 characters in length that contains only letters, digits, spaces, or the following characters:</p> <p>- ( ) + , . / : ?</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>

Table 47. *ldapcfg* command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<p><b>Set LDAP login permission attribute</b></p>	<p>Sets the login permission attribute that is used to determine retrieve user permissions on the LDAP server.</p> <p><b>Note:</b> For a login permission attribute to be used, LDAP security must be set to v1 using the <b>-v</b> command option.</p>	<p><code>ldapcfg -lpa "permission"</code> where "permission" is a quote-delimited string of up to 23 characters in length that contains only letters, digits, spaces, or the following characters:</p> <p style="padding-left: 40px;">- ( ) + , . / : ?</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p style="padding-left: 40px;">mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>
<p><b>Set LDAP name</b></p>	<p>Sets the LDAP name for the CMM.</p> <p><b>Note:</b> For an LDAP name to be used, LDAP security must be set to v2 using the <b>-v</b> command option.</p>	<p><code>ldapcfg -t name</code> where name is an alphanumeric string up to 63 characters in length containing any character except for angle brackets (&lt; and &gt;) and spaces.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p style="padding-left: 40px;">mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>

Table 47. *ldapcfg* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Set LDAP server discovery method</b></p>	<p>Sets the method to use for discovering LDAP servers that provide user authentication.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• If the <code>dns</code> method is specified, the following values must also be set: <ul style="list-style-type: none"> <li>– A domain name using the <code>-dn</code> command option.</li> <li>– A forest name using the <code>-fn</code> command option.</li> </ul> </li> <li>• If the <code>preconf</code> method is specified, the following values must also be set: <ul style="list-style-type: none"> <li>– An LDAP server hostname or IP address using the <code>-i1</code>, <code>-i2</code>, <code>-i3</code>, and <code>-i4</code> command options.</li> <li>– A port for each LDAP server hostname or IP address using the <code>-p1</code>, <code>-p2</code>, <code>-p3</code>, and <code>-p4</code> command options.</li> </ul> </li> </ul>	<p><code>ldapcfg -server <i>method</i></code>  where <i>method</i> is:</p> <ul style="list-style-type: none"> <li>• <code>dns</code> for dynamic discovery</li> <li>• <code>preconf</code> to use an LDAP server that was manually pre-configured</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>  where <i>x</i> is the primary CMM bay number.</p>
<p><b>Set LDAP server domain name</b></p>	<p>Sets the search domain to use for Domain Controller (DC) dynamic discovery.</p>	<p><code>ldapcfg -dn <i>domain</i></code>  where <i>domain</i> is an alphanumeric string up to 255 characters in length.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>  where <i>x</i> is the primary CMM bay number.</p>
<p><b>Set LDAP server forest name</b></p>	<p>Sets the forest name to use for Global Catalog (GC) dynamic discovery.</p>	<p><code>ldapcfg -fn <i>forestname</i></code>  where <i>forestname</i> is an alphanumeric string up to 63 characters in length.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>  where <i>x</i> is the primary CMM bay number.</p>

Table 47. *ldapcfg* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>First LDAP server host name or IP address - set</b>	Checks syntax and sets the first LDAP server host name or IP address to use for pre-configured LDAP server discovery. <b>Note:</b> A port for this LDAP server hostname or IP address must be set using the <b>-p1</b> command option.	<code>ldapcfg -i1 hostname/ip_ address</code> where <i>hostname/ip_ address</i> is the first host name or IP address, up to 255 characters in length.  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Second LDAP server host name or IP address - set</b>	Checks syntax and sets the second LDAP server host name or IP address to use for pre-configured LDAP server discovery. <b>Note:</b> A port for this LDAP server hostname or IP address must be set using the <b>-p2</b> command option.	<code>ldapcfg -i2 hostname/ip_ address</code> where <i>hostname/ip_ address</i> is the second host name or IP address, up to 255 characters in length.  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Third LDAP server host name or IP address - set</b>	Checks syntax and sets the third LDAP server host name or IP address to use for pre-configured LDAP server discovery. <b>Note:</b> A port for this LDAP server hostname or IP address must be set using the <b>-p3</b> command option.	<code>ldapcfg -i3 hostname/ip_ address</code> where <i>hostname/ip_ address</i> is the third host name or IP address, up to 255 characters in length.  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 47. *ldapcfg* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Fourth LDAP server host name or IP address - set</b>	Checks syntax and sets the fourth LDAP server host name or IP address to use for pre-configured LDAP server discovery. <b>Note:</b> A port for this LDAP server hostname or IP address must be set using the <b>-p4</b> command option.	<code>ldapcfg -i4 <i>hostname/ip_address</i></code> where <i>hostname/ip_address</i> is the fourth host name or IP address, up to 255 characters in length.  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>First LDAP server port number - set</b>	Sets the port number of the first LDAP server to use for pre-configured LDAP server discovery.	<code>ldapcfg -p1 <i>port</i></code> where <i>port</i> is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Second LDAP server port number - set</b>	Sets the port number of the second LDAP server to use for pre-configured LDAP server discovery.	<code>ldapcfg -p2 <i>port</i></code> where <i>port</i> is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 47. *ldapcfg* command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Third LDAP server port number - set</b>	Sets the port number of the third LDAP server to use for preconfigured LDAP server discovery.	<p><code>ldapcfg -p3 port</code>            where <i>port</i> is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  <code>mm[p]</code> <code>mm[P]</code> <code>mm[x]</code> where <i>x</i> is the primary CMM bay number.
<b>Fourth LDAP server port number - set</b>	Sets the port number of the fourth LDAP server to use for preconfigured LDAP server discovery.	<p><code>ldapcfg -p4 port</code>            where <i>port</i> is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  <code>mm[p]</code> <code>mm[P]</code> <code>mm[x]</code> where <i>x</i> is the primary CMM bay number.
<b>Set LDAP root distinguished name</b>	Sets the root distinguished name for the root entry of the LDAP directory tree that is used as the base object for all searches.	<p><code>ldapcfg -rd "name"</code>            where "<i>name</i>" is up to 255 characters in length and contained within double-quotes. Names can contain any character, including spaces.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  <code>mm[p]</code> <code>mm[P]</code> <code>mm[x]</code> where <i>x</i> is the primary CMM bay number.

Table 47. *ldapcfg* command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<p><b>Set LDAP UID search attribute</b></p>	<p>Sets the UID search attribute that represents the user IDs stored on the LDAP server.</p> <p>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".</p>	<p><code>ldapcfg -usa "UID"</code>            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 "?".</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>
<p><b>Set LDAP server binding method</b></p>	<p>Sets the binding method for initial connection to the LDAP server.</p> <p><b>Notes:</b> If the binding method is set to cc, the following values must also be set:</p> <ul style="list-style-type: none"> <li>• A UID search attribute using the <code>-usa</code> command option</li> <li>• A client distinguished name using the <code>-cd</code> command option.</li> <li>• A client password using the <code>-p</code> and <code>-cp</code> command options.</li> </ul>	<p><code>ldapcfg -bm method</code>            where <i>method</i> is:</p> <ul style="list-style-type: none"> <li>• cc for configured credentials</li> <li>• lc for login credentials</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>
<p><b>Set LDAP server to be used for authentication only</b></p>	<p>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.</p>	<p><code>ldapcfg -aom state</code>            where <i>state</i> is enabled or disabled</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>

Table 47. *ldapcfg* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Set LDAP client distinguished name</b>	Sets the client distinguished name (DN) for initial connection to the LDAP server. <b>Note:</b> A client password must also be set using the <code>-p</code> and <code>-cp</code> command options.	<code>ldapcfg -cd domain</code> where <i>domain</i> is an alphanumeric string up to 255 characters in length containing any character except for angle brackets ( < and > ) and spaces.  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Set LDAP client distinguished name password</b>	Sets the client distinguished name password for initial connection to the LDAP server. <b>Note:</b> The passwords must be specified by both the <code>-p</code> and <code>-cp</code> command options and must match.	<code>ldapcfg -p password</code> where <i>password</i> is an alphanumeric string up to 15 characters in length.  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Set (confirm) LDAP client distinguished name password</b>	Sets, for confirmation purposes, the client distinguished name password for initial connection to the LDAP server. <b>Note:</b> The passwords must be specified by both the <code>-p</code> and <code>-cp</code> command options and must match.	<code>ldapcfg -cp password</code> where <i>password</i> is an alphanumeric string up to 15 characters in length.  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

**Example:**

To display the CMM LDAP settings, while the Flex System Enterprise 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 Flex System Enterprise 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 385 for a list of error messages that apply to all commands or “led command errors” on page 423 for a list of error messages that are specific to the led command.

Table 48. led command

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Display LED states for chassis</b>	Displays various LED states for the chassis.	led	Flex System Enterprise Chassis: system
<b>Display fault LED state for chassis</b>	Displays fault LED state for the chassis.	led	Primary CMM: mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Display state for compute node LEDs</b>	Displays the state of the compute node LEDs.	led	Compute node: blade[x] where x is the node bay number.
<b>Display state for rear LED card LEDs</b>	Displays the state of the rear LED card LEDs of the Flex System Enterprise Chassis.	led	Rear LED card: mt[x] where x is the rear LED card.
<b>Display state for fanpack LEDs</b>	Displays the state of the fan pack LEDs of the Flex System Enterprise Chassis.	led	Power supply fan pack: power[x] where x is the power supply (fan pack) bay number.
<b>Display state for fan logic module LEDs</b>	Displays the state of the fan logic module LEDs of the Flex System Enterprise Chassis.	led	Fan logic module: fanmux[x] where x is the fan logic module bay number.
<b>Display state for fan module fault LED</b>	Displays the state of the fan module fault LED of the Flex System Enterprise Chassis.	led	Fan module: blower[x] where x is the fan module bay number.
<b>Display state for I/O module LEDs</b>	Displays state of the LEDs for the specified I/O module.	led	I/O module: switch[x] where x is the I/O-bay number.

Table 48. led command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Turn off information LED</b>	Turns off the information LED, that is on the Flex System Enterprise Chassis and some components, for the specified command target	led -info off This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis administration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Flex System Enterprise Chassis: system  Compute node: blade[x] where x is the node bay number.  Rear LED card: mt[x] where x is the rear LED card.
<b>Set identify LED state</b>	Sets the state of the identify LED, that is on the Flex System Enterprise Chassis and some compute nodes and I/O modules, for the command target.	led -loc state where state is <ul style="list-style-type: none"> <li>• on</li> <li>• off</li> <li>• blink</li> </ul> <b>Note:</b> A state of blink can only be used for the system and mt command targets and for the compute nodes.  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis administration (for Flex System Enterprise Chassis)</li> <li>• Blade administration (for compute node)</li> <li>• I/O module administration (for I/O modules)</li> </ul> See “Commands and user authority” on page 10 for additional information.	Flex System Enterprise Chassis: system  Rear LED card: mt[x] where x is the rear LED card.  Compute node: blade[x] where x is the node bay number.  I/O module: switch[x] where x is the I/O-bay number.

**Example:**To display the LED status for the compute node in bay 2, while the Flex System Enterprise 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 Flex System Enterprise Chassis, including how many CMMs are installed in the Flex System Enterprise 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 385 for a list of error messages that apply to all commands or “list command errors” on page 424 for a list of error messages that are specific to the list command.

Table 49. list command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>View command target</b>	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.
<b>View system configuration tree</b>	Displays the tree structure of devices present in the Flex System Enterprise 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 <i>depth</i> where <i>depth</i> is <ul style="list-style-type: none"> <li>• all or a for full tree display, starting at the command target level</li> <li>• 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.</li> </ul>	Any installed device.

**Example:** To display a list of devices installed in the Flex System Enterprise Chassis, while the Flex System Enterprise 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 385 for a list of error messages that apply to all commands or “monalerts command errors” on page 424 for a list of error messages that are specific to the monalerts command.

Table 50. monalerts command

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Display monitored alert states</b>	Displays the state of all alerts being monitored by the CMM.	monalerts	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Set state for enhanced legacy alert categories</b>	Enables enhanced legacy alert categories. <ul style="list-style-type: none"> <li>• If enhanced legacy alert categories are enabled, alerts are configured using the monalerts command.</li> <li>• If enhanced legacy alert categories can not be disabled once they have been enabled.</li> </ul>	monalerts -ec <i>state</i> where <i>state</i> is enabled .  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Set monitoring state for all critical alerts</b>	Enables or disables monitoring of all critical alerts.	monalerts -ca <i>state</i> where <i>state</i> is enabled or disabled .  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Set monitoring state for node device critical alerts</b>	Enables or disables monitoring of node device critical alerts.	monalerts -cb <i>state</i> where <i>state</i> is enabled or disabled .  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 50. monalerts command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Set monitoring state for I/O-module critical alerts</b>	Enables or disables monitoring of I/O-module critical alerts.	<p>monalerts -ciom <i>state</i>            where <i>state</i> is enabled or disabled .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>
<b>Set monitoring state for chassis or system management critical alerts</b>	Enables or disables monitoring of chassis or system management critical alerts.	<p>monalerts -ccsm <i>state</i>            where <i>state</i> is enabled or disabled .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>
<b>Set monitoring state for cooling device critical alerts</b>	Enables or disables monitoring of cooling device critical alerts.	<p>monalerts -ccd <i>state</i>            where <i>state</i> is enabled or disabled .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>

Table 50. monalerts command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Set monitoring state for power supply critical alerts</b>	Enables or disables monitoring of power supply critical alerts.	monalerts -cpm <i>state</i> where <i>state</i> is enabled or disabled .  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Set monitoring state for all warning alerts</b>	Enables or disables monitoring of all warning alerts.	monalerts -wa <i>state</i> where <i>state</i> is enabled or disabled .  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Set monitoring state for node device warning alerts</b>	Enables or disables monitoring of node device warning alerts.	monalerts -wb <i>state</i> where <i>state</i> is enabled or disabled .  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.



Table 50. monalerts command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Set monitoring state for I/O-module warning alerts</b>	Enables or disables monitoring of I/O-module warning alerts.	<p>monalerts -wiom <i>state</i> where <i>state</i> is enabled or disabled .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>
<b>Set monitoring state for chassis or system management warning alerts</b>	Enables or disables monitoring of chassis or system management warning alerts.	<p>monalerts -wscm <i>state</i> where <i>state</i> is enabled or disabled .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>
<b>Set monitoring state for event log warning alerts</b>	Enables or disables monitoring of event log warning alerts.	<p>monalerts -wel <i>state</i> where <i>state</i> is enabled or disabled .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>

Table 50. monalerts command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Set monitoring state for cooling device warning alerts</b>	Enables or disables monitoring of cooling device warning alerts.	<p>monalerts -wcd <i>state</i>            where <i>state</i> is enabled or disabled .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>
<b>Set monitoring state for power supply warning alerts</b>	Enables or disables monitoring of power supply warning alerts.	<p>monalerts -wpm <i>state</i>            where <i>state</i> is enabled or disabled .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>
<b>Set monitoring state for all informational alerts</b>	Enables or disables monitoring of all informational alerts.	<p>monalerts -ia <i>state</i>            where <i>state</i> is enabled or disabled .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>

Table 50. monalerts command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Set monitoring state for node device informational alerts</b>	Enables or disables monitoring of node device informational alerts.	<p>monalerts -ib <i>state</i>            where <i>state</i> is enabled or disabled .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>
<b>Set monitoring state for I/O-module informational alerts</b>	Enables or disables monitoring of I/O-module informational alerts.	<p>monalerts -iioM <i>state</i>            where <i>state</i> is enabled or disabled .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>
<b>Set monitoring state for chassis or system management informational alerts</b>	Enables or disables monitoring of chassis or system management informational alerts.	<p>monalerts -icsm <i>state</i>            where <i>state</i> is enabled or disabled .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>

Table 50. monalerts command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Set monitoring state for power state informational alerts</b>	Enables or disables monitoring of power state (on/off) informational alerts.	monalerts -ipon <i>state</i> where <i>state</i> is enabled or disabled .  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Set monitoring state for inventory change informational alerts</b>	Enables or disables monitoring of inventory change (installed components) informational alerts.	monalerts -iinv <i>state</i> where <i>state</i> is enabled or disabled .  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Set monitoring state for event log informational alerts</b>	Enables or disables monitoring of event log informational alerts.	monalerts -iel <i>state</i> where <i>state</i> is enabled or disabled .  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 50. monalerts command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Set monitoring state for network change informational alerts</b>	Enables or disables monitoring of network change informational alerts.	monalerts -inc <i>state</i> where <i>state</i> is enabled or disabled .  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Set monitoring state for user activity informational alerts</b>	Enables or disables monitoring of user activity informational alerts.	monalerts -iua <i>state</i> where <i>state</i> is enabled or disabled .  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 50. monalerts command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Set monitoring state for cooling device informational alerts</b>	Enables or disables monitoring of cooling device informational alerts.	<p>monalerts -icd <i>state</i>            where <i>state</i> is enabled or disabled .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Set monitoring state for power supply informational alerts</b>	Enables or disables monitoring of power supply informational alerts.	<p>monalerts -ipm <i>state</i>            where <i>state</i> is enabled or disabled .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	Primary CMM:  mm[p] mm[P] mm[x] 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 Flex System Enterprise 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 385 for a list of error messages that apply to all commands or “ntp command errors” on page 424 for a list of error messages that are specific to the ntp command.

Table 51. ntp command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display NTP settings</b>	<p>Displays the NTP settings for the specified command target. Possible return values are:</p> <ul style="list-style-type: none"> <li>• <code>-en state</code> (enabled, disabled)</li> <li>• <code>-i ipaddress/hostname</code> (IP address or hostname of the NTP server)</li> <li>• <code>-f update_frequency</code> (NTP update frequency, in minutes)</li> <li>• <code>-v3en state</code> (enabled, disabled)</li> <li>• <code>-v3 key_info</code> (NTP v3 authentication entry)</li> </ul> <p><b>Note:</b> Return values vary based on command target.</p>	ntp	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p> <p>I/O module:</p> <p>switch[x] where x is the I/O-bay number.</p>
<b>Enable / disable NTP</b>	<p>Enables or disables NTP for the specified command target. For I/O module targets, the <code>ntp -en</code> 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.</p>	<p><code>ntp -en state</code> where <i>state</i> is enabled or disabled.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p> <p>I/O module:</p> <p>switch[x] where x is the I/O-bay number.</p>
<b>NTP server IP address or hostname - set</b>	<p>Checks syntax and sets the IP address or hostname of the NTP server.</p>	<p><code>ntp -i ipaddress/hostname</code> where <i>ipaddress/hostname</i> is the IP address or hostname of the NTP server.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>

Table 51. ntp command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<p><b>NTP update frequency - set</b></p>	<p>Sets how often the clock in the specified command target is automatically updated by the NTP server.</p>	<p><code>ntp -f time</code>            where <i>time</i> is the NTP update frequency, in minutes with a maximum value of 45000.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where <i>x</i> is the primary CMM bay number.</p> <p>I/O module:</p> <p><code>switch[x]</code>            where <i>x</i> is the I/O-bay number.</p>
<p><b>NTP - Enable / disable V3 authentication</b></p>	<p>Enables or disables V3 authentication between the CMM and the NTP server.</p> <p><b>Note:</b> The NTP server authentication key must be set, using the <code>ntp -v3</code> command option, before enabling V3 authentication.</p>	<p><code>ntp -v3en state</code>            where <i>state</i> is enabled or disabled .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where <i>x</i> is the primary CMM bay number.</p>



Table 51. ntp command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>NTP server authentication key - set</b>	<p>Sets the v3 authentication key that the CMM uses to access the NTP server. The authentication key contains the following values:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Key type: The CMM supports only the SHA1 key type.</li> <li>• Key: The key is an 40-character ASCII string.</li> <li>• The <code>ntp -v3key_index</code> and <code>key</code> 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.</li> </ul>	<p><code>ntp -v3 key_indexkey_typekey</code> where:</p> <ul style="list-style-type: none"> <li>• <code>key_index</code> is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.</li> <li>• <code>key_type</code> is SHA1.</li> <li>• <code>key</code> is a 40-character ASCII string.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>
<b>NTP clock-synchronize</b>	<p>Synchronizes the CMM clock with the NTP server. (You must configure a valid NTP server before you can synchronize.)</p>	<p><code>ntp -synch</code> This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>

**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]>
```

---

## permggroups command

This command displays and configures user permission groups of the primary CMM.

**Important:** Users and permission groups for the Flex System Enterprise Chassis are controlled by the CMM in each Flex System Enterprise Chassis, using the CMM CLI “users command” on page 353 and the “permggroups command” on page 228 or the CMM web interface. If your Flex System configuration includes optional Flex System Manager hardware, users and permission groups for each optional Flex System Manager installation are controlled by the optional Flex System Manager software (see [http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.8731.doc/product\\_page.html](http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.8731.doc/product_page.html) for information).

### Notes:

- Permission groups are assigned to users using the “users command” on page 353.
- Permission groups can be backed up as part of the CMM configuration using the “write command” on page 383.
- Permission groups are restored as part of a backed up CMM configuration using the “read command” on page 269.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See “Common errors” on page 385 for a list of error messages that apply to all commands or “permggroups command errors” on page 425 for a list of error messages that are specific to the permggroups command.

Table 52. *permggroups command*

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display all user permission groups</b>	Displays all user permission groups set up for the CMM.	permggroups	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Display specific user permission group</b>	Displays information for the specified user permission group.	permggroups -n <i>group_name</i> where <i>group_name</i> is the name that identifies the user permission group.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 52. `permggroups` command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<p><b>Add user permission group</b></p>	<p>Creates a new user permission group.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• User permission group names can not be changed after they are added.</li> <li>• Group names are not case sensitive.</li> </ul>	<p><code>permggroups -add -n group_name -a group_authority</code>            where:</p> <ul style="list-style-type: none"> <li>• <code>group_name</code> 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.</li> <li>• <code>group_authority</code> uses the following syntax:               <ul style="list-style-type: none"> <li>- <code>operator (Operator)</code></li> <li>- <code>rbs:roles:scope</code> where the <i>roles</i> are one or more of the following authority levels, separated by a vertical bar ( ):                   <ul style="list-style-type: none"> <li>- <code>super (Supervisor)</code></li> <li>- <code>cam (Chassis User Account Management)</code></li> <li>- <code>clm (Chassis Log Management)</code></li> <li>- <code>co (Chassis Operator)</code></li> <li>- <code>cc (Chassis Configuration)</code></li> <li>- <code>ca (Chassis Administration)</code></li> <li>- <code>bo (Blade Operator)</code></li> <li>- <code>brp (Blade Remote Present)</code></li> <li>- <code>bc (Blade Configuration)</code></li> <li>- <code>ba (Blade Administration)</code></li> <li>- <code>so (I/O Module Operator)</code></li> <li>- <code>sc (I/O Module Configuration)</code></li> <li>- <code>sa (I/O Module Administration)</code></li> </ul> </li> </ul> <p><i>(continued on next page)</i></p> </li></ul>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where x is the primary CMM bay number.</p>
<p><b>Add user permission group</b>  <i>(continued)</i></p>		<p>where the <i>scope</i> is one or more of the following devices, separated by a vertical bar ( ). Ranges of devices are separated by a dash (-).</p>	

Table 52. *permggroups* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
		<ul style="list-style-type: none"> <li>• <i>c n</i> (Chassis <i>n</i>, where <i>n</i> is 1)</li> <li>• <i>b n</i> (Blade <i>n</i>, where <i>n</i> is a valid node bay number in the chassis)</li> <li>• <i>s n</i> (I/O module <i>n</i>, where <i>n</i> is a valid I/O-bay number in the chassis)</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	
<p><b>Modify user permission group</b></p>	<p>Modify the selected user permission group.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• User permission group names can not be changed after they are added.</li> <li>• Group names are not case sensitive.</li> </ul>	<p><code>permggroups -n <i>group_name</i> -a <i>group_authority</i></code>            where:</p> <ul style="list-style-type: none"> <li>• <i>group_name</i> is the name that identifies the user permission group.</li> <li>• <i>group_authority</i> uses the following syntax:               <ul style="list-style-type: none"> <li>– <code>operator</code> (Operator)</li> <li>– <code>rbs:roles:scope</code> where the <i>roles</i> are one or more of the following authority levels, separated by a vertical bar ( ):                   <ul style="list-style-type: none"> <li>– <code>super</code> (Supervisor)</li> <li>– <code>cam</code> (Chassis User Account Management)</li> <li>– <code>clm</code> (Chassis Log Management)</li> <li>– <code>co</code> (Chassis Operator)</li> <li>– <code>cc</code> (Chassis Configuration)</li> <li>– <code>ca</code> (Chassis Administration)</li> <li>– <code>bo</code> (Blade Operator)</li> <li>– <code>brp</code> (Blade Remote Present)</li> <li>– <code>bc</code> (Blade Configuration)</li> </ul> </li> </ul> </li> </ul>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where <i>x</i> is the primary CMM bay number.</p>

Table 52. `permggroups` command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
		<ul style="list-style-type: none"> <li>- ba (Blade Administration)</li> <li>- so (I/O Module Operator)</li> <li>- sc (I/O Module Configuration)</li> <li>- sa (I/O Module Administration)</li> </ul> <p>(continued on next page)</p>	
<p><b>Modify user permission group</b> (continued)</p>		<p>where the <i>scope</i> is one or more of the following devices, separated by a vertical bar ( ). Ranges of devices are separated by a dash (-).</p> <ul style="list-style-type: none"> <li>• <i>c n</i> (Chassis <i>n</i>, where <i>n</i> is 1)</li> <li>• <i>b n</i> (Blade <i>n</i>, where <i>n</i> is a valid node bay number in the chassis)</li> <li>• <i>s n</i> (I/O module <i>n</i>, where <i>n</i> is a valid I/O-bay number in the chassis)</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	
<p><b>Delete user permission group</b></p>	<p>Delete the specified user permission group. <b>Note:</b> Group names are not case sensitive.</p>	<p><code>permggroups -n <i>group_name</i> -clear</code> where <i>group_name</i> is the name that identifies the user permission group.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code> <code>mm[P]</code> <code>mm[x]</code> where <i>x</i> is the primary CMM bay number.</p>

**Example:** To add a user permission group with a name of superuser that has supervisor rights to all Flex System components, while the Flex System Enterprise Chassis is set as the persistent command environment, at the `system >` prompt, type

```
permggroups -add -n superuser -a rbs:super:c1|b1-b14|s1-s4 -T mm[p]
```

To display information for the superuser group, while the Flex System Enterprise Chassis is set as the persistent command environment, at the `system >` prompt, type

```
permggroups -n superuser -T mm[p]
```

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

```
system> permggroups -add -n superuser -a rbs:super:c1|b1-b14|s1-s4 -T mm[p]
```

```
OK
```

```
system> permggroups -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 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 385 for a list of error messages that apply to all commands or “ping command errors” on page 426 for a list of error messages that are specific to the ping command.

Table 53. ping command

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Display IP addresses</b>	Displays a list of index numbers and IP addresses for the specified command target.	ping -i	Compute node:  blade[x] where x is the node bay number.  I/O module:  switch[x] where x is the I/O-bay number.
<b>Ping compute node IP address</b>	Pings the specified compute node IP address to test communication between the compute node and the CMM.	ping -i <i>ip_address</i> where <i>ip_address</i> is the IP address to ping. <b>Note:</b> Valid index numbers and IP addresses for components installed in the Flex System Enterprise Chassis can be seen by running the ping -i command, directed to a specific command target with no arguments.	Compute node:  blade[x] where x is the node bay number.
<b>Ping I/O-module IP address</b>	Pings the specified I/O-module IP address to test communication between the I/O module and the CMM.	ping -i <i>ip_address</i> where <i>ip_address</i> is the IP address to ping. <b>Note:</b> Valid index numbers and IP addresses for components installed in the Flex System Enterprise Chassis can be seen by running the ping -i command, directed to a specific command target with no arguments.	I/O module:  switch[x] where x is the I/O-bay number.

Table 53. ping command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Ping compute node IP address</b>	Pings the specified compute node to test communication.	ping -i <i>index</i> where <i>index</i> is the index number for the compute node IP address to ping. <b>Note:</b> Valid index numbers and IP addresses for components installed in the Flex System Enterprise Chassis can be seen by running the ping -i command, directed to a specific command target with no arguments.	Compute node:  blade[x] where x is the node bay number.
<b>Ping I/O-module IP address</b>	Pings the specified I/O module to test communication.	ping -i <i>index</i> where <i>index</i> is the index number for the I/O-module IP address to ping. <b>Note:</b> Valid index numbers and IP addresses for components installed in the Flex System Enterprise Chassis can be seen by running the ping -i command, directed to a specific command target with no arguments.	I/O module:  switch[x] where x is the I/O-bay number.

**Example:** To display the IP addresses of the I/O module in bay 2, while the Flex System Enterprise 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 Flex System Enterprise 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 Flex System Enterprise 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 Flex System Enterprise 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 385 for a list of error messages that apply to all commands or “pmpolicy command errors” on page 427 for a list of error messages that are specific to the pmpolicy command.

Table 54. *pmpolicy* command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display current power management policy</b>	Displays the current power management policy.	<code>pmpolicy</code>	Flex System Enterprise Chassis: system
<b>Display current and available power management policies</b>	Displays both the current and available power management policies.	<code>pmpolicy pd</code>	Flex System Enterprise Chassis: system
<b>Set power management policy</b>	Set power management policy.	<p><code>pmpolicy -pm <i>policy</i></code> or</p> <p><code>pmpolicy pd -pm <i>policy</i></code></p> <p>where <i>policy</i> is:</p> <ul style="list-style-type: none"> <li>• <code>acred</code> (ac power source redundancy policy)</li> <li>• <code>acredov</code> (ac power source redundancy policy, with compute node throttling)</li> <li>• <code>redwperf</code> (power supply redundancy, no compute node oversubscription)</li> <li>• <code>redwperf</code> (power supply redundancy with compute node power throttling)</li> <li>• <code>nonred</code> (no power management policy)</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	Flex System Enterprise Chassis: 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 385 for a list of error messages that apply to all commands or “portcfg command errors” on page 427 for a list of error messages that are specific to the portcfg command.

Table 55. portcfg command

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Display CMM serial port configuration</b>	Displays the current configuration of the CMM serial port. Possible return values are: <ul style="list-style-type: none"> <li>• -b <i>baud_rate</i></li> <li>• -p <i>parity</i></li> <li>• -s <i>stop_bits</i></li> </ul>	portcfg -com1	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Set CMM serial port baud rate</b>	Checks syntax and sets the baud (communications) rate of the CMM serial port.	portcfg -com1 -b <i>baud_rate</i> where <i>baud_rate</i> is 2400, 4800, 9600, 19200, 38400, 57600, or 115200.  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 55. portcfg command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Set CMM serial port parity</b>	Checks syntax and sets the parity of the CMM serial port.	<pre>portcfg -com1 -p <i>parity</i></pre> where <i>parity</i> is <ul style="list-style-type: none"> <li>• none</li> <li>• odd</li> <li>• even</li> <li>• mark</li> <li>• space</li> </ul> This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM: mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Set CMM serial port stop bits</b>	Checks syntax and sets the number of stop bits for the CMM serial port. <b>Note:</b> When 2 stop bits is selected, the software automatically adjusts between 1.5 and 2 stop bits, based on the detected data-word size.	<pre>portcfg -com1 -s <i>stop_bits</i></pre> where <i>stop_bits</i> is: <ul style="list-style-type: none"> <li>• 1 for 1 stop bit.</li> <li>• 2 for 1.5 or 2 stop bits.</li> </ul> This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM: mm[p] mm[P] mm[x] 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.

**Note:** Changes to the `-ftpe`, `-snmp1ae`, `-snmp3ae`, `-snmp1te`, `-sshe`, `-ftpp`, `-ftpdp`, `-http`, `-https`, `-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.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See “Common errors” on page 385 for a list of error messages that apply to all commands or “ports command errors” on page 427 for a list of error messages that are specific to the ports command.

**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 56. ports command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Display network port settings</b></p>	<p>Displays the network port settings for the CMM. Returned values are:</p> <ul style="list-style-type: none"> <li>• -cimp <i>cim_prt_num</i></li> <li>• -ftpp <i>FTP_prt_num</i></li> <li>• -ftpdp <i>FTP_data_prt_num</i></li> <li>• -http <i>HTTP_prt_num</i></li> <li>• -https <i>HTTPS_prt_num</i></li> <li>• -slpp <i>SLP_prt_num</i></li> <li>• -snmpap <i>SNMP_agent_prt_num</i></li> <li>• -snmptp <i>SNMP_traps_prt_num</i></li> <li>• -sshp <i>SSH_prt_num</i></li> <li>• -stcmp <i>secure_tcmp</i></li> <li>• -tcmp <i>TCP_cmd_md_port</i></li> <li>• -telnetp <i>Telnet_prt_num</i></li> <li>• -tftpp <i>TFTP_prt_num</i></li> <li>• -cime <i>cim_prt_state</i></li> <li>• -ftpe <i>FTP_state</i></li> <li>• -sftpe <i>sec_FTP_state</i></li> <li>• -httpse <i>HTTPS_prt_state</i></li> <li>• -ntpe <i>NTP_state</i></li> <li>• -slpe <i>SLP_state</i>.</li> <li>• -snmp1ae <i>SNMPv1_agent_state</i></li> <li>• -snmp3ae <i>SNMPv3_agent_state</i></li> <li>• -snmpte <i>SNMP_traps_state</i></li> <li>• -sshe <i>SSH_prt_state</i></li> <li>• -stcme <i>secure_TCP_cmd_mode</i></li> <li>• -tcme <i>TCP_cmd_mode_state</i></li> <li>• -telnete <i>Telnet_prt_state-</i></li> <li>• -tftpe <i>TFTP_state</i></li> <li>• -ftpt <i>FTP_timeout</i></li> <li>• -tcmt <i>TCP_cmd_mode_timeout</i></li> <li>• -telnett <i>Telnet_prt_timeout</i></li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• The following will not be available if the CMM chassis security level is set to secure with the “security command” on page 287: <ul style="list-style-type: none"> <li>– HTTP</li> <li>– FTP</li> <li>– SNMPv1</li> <li>– Telnet</li> <li>– TFTP</li> <li>– Non-secure TCP command mode</li> </ul> </li> <li>• HTTPSE can only be disabled by disabling all web access using the “uicfg command” on page 339.</li> </ul>	<p>ports</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>
<p><b>Display open CMM ports</b></p>	<p>Displays the CMM ports that are currently open.</p> <p><b>Notes:</b> The following will not be available if the CMM security level is set to secure with the “security command” on page 287:</p> <ul style="list-style-type: none"> <li>• HTTP</li> </ul>	<p>ports -open</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x]</p>

Table 56. ports command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
	<ul style="list-style-type: none"> <li>• FTP</li> <li>• SNMPv1</li> <li>• Telnet</li> <li>• TFTP</li> <li>• Non-secure TCP command mode</li> </ul>		<p>where <i>x</i> is the primary CMM bay number.</p>
<b>Reset network port settings</b>	<p>Resets all network port settings for the CMM to the default values. Default values are:</p> <ul style="list-style-type: none"> <li>• -ftpp: 21</li> <li>• -ftpdp: 20</li> <li>• -cimp: 5989</li> <li>• -http: 80</li> <li>• -httpsp: 443</li> <li>• -slpp: 427</li> <li>• -tcmp: 6090</li> <li>• -snmpap: 161</li> <li>• -snmptp: 162</li> <li>• -sshp: 22</li> <li>• -stcmp: 6091</li> <li>• -telnetp: 23</li> <li>• -tftpp: 69</li> </ul> <p><b>Notes:</b> The following will not be available if the CMM security level is set to secure with the “security command” on page 287:</p> <ul style="list-style-type: none"> <li>• HTTP</li> <li>• FTP</li> <li>• SNMPv1</li> <li>• Telnet</li> <li>• TFTP</li> <li>• Non-secure TCP command mode</li> </ul>	<p>ports -reset</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where <i>x</i> is the primary CMM bay number.</p>
<b>Set FTP port number</b>	<p>Sets the port number for the CMM FTP port.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• The FTP port will not be available if the CMM chassis security level is set to secure with the “security command” on page 287.</li> <li>• You cannot configure a port to a number that is already in use.</li> <li>• Changes to port numbers take effect immediately.</li> <li>• Changing port numbers will affect ongoing operations using the service at that port.</li> </ul>	<p>ports -ftpp <i>FTPprt_num</i> where <i>FTPprt_num</i> is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where <i>x</i> is the primary CMM bay number.</p>



Table 56. ports command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Set FTP data port number</b>	<p>Sets the port number for the CMM FTP data port.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>The FTP data port will not be available if the CMM chassis security level is set to secure with the “security command” on page 287.</li> <li>You cannot configure a port to a number that is already in use.</li> <li>Changes to port numbers take effect immediately.</li> <li>Changing port numbers will affect ongoing operations using the service at that port.</li> </ul>	<p>ports -ftpdp <i>FTP_dataprt_num</i>            where <i>FTP_dataprt_num</i> is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>
<b>Set HTTP port number</b>	<p>Sets the port number for the CMM HTTP port.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>The HTTP port will not be available if the CMM security level is set to secure with the “security command” on page 287.</li> <li>You cannot configure a port to a number that is already in use.</li> <li>Changes to port numbers take effect immediately.</li> <li>Changing port numbers will affect ongoing operations using the service at that port.</li> </ul>	<p>ports -http <i>HTTPprt_num</i>            where <i>HTTPprt_num</i> is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>
<b>Set HTTPS port number</b>	<p>Sets the port number for the CMM HTTPS port.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>You cannot configure a port to a number that is already in use.</li> <li>Changes to port numbers take effect immediately.</li> <li>Changing port numbers will affect ongoing operations using the service at that port.</li> </ul>	<p>ports -https <i>HTTPSprt_num</i>            where <i>HTTPSprt_num</i> is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>

Table 56. ports command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Set CIM port number over HTTPS</b></p>	<p>Sets the port number for using the CMM common information model (CIM) over HTTPS.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>You cannot configure a port to a number that is already in use.</li> <li>Changes to port numbers take effect immediately.</li> <li>Changing port numbers will affect ongoing operations using the service at that port.</li> </ul>	<p><code>ports -cimp <i>cimprt_num</i></code>            where <i>cimprt_num</i> is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where <i>x</i> is the primary CMM bay number.</p>
<p><b>Set SLP port number</b></p>	<p>Sets the SLP port number.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>You cannot configure a port to a number that is already in use.</li> <li>Changes to port numbers take effect immediately.</li> <li>Changing port numbers will affect ongoing operations using the service at that port.</li> </ul>	<p><code>ports -slpp <i>SLPprt_num</i></code>            where <i>SLPprt_num</i> is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where <i>x</i> is the primary CMM bay number.</p>
<p><b>Set SNMP agent port number</b></p>	<p>Sets the port number for the CMM SNMP agent port.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>SNMPv1 ports will not be available if the CMM security level is set to secure with the “security command” on page 287.</li> <li>You cannot configure a port to a number that is already in use.</li> <li>Changes to port numbers take effect immediately.</li> <li>Changing port numbers will affect ongoing operations using the service at that port.</li> </ul>	<p><code>ports -snmpap <i>SNMPagentprt_num</i></code>            where <i>SNMPagentprt_num</i> is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where <i>x</i> is the primary CMM bay number.</p>

Table 56. ports command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<p><b>Set SNMP traps port number</b></p>	<p>Sets the port number for the CMM SNMP traps port.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• SNMPv1 ports will not be available if the CMM security level is set to secure with the "security command" on page 287.</li> <li>• You cannot configure a port to a number that is already in use.</li> <li>• Changes to port numbers take effect immediately.</li> <li>• Changing port numbers will affect ongoing operations using the service at that port.</li> </ul>	<p>ports -snmptp <i>SNMP_trapsprt_num</i>            where <i>SNMP_trapsprt_num</i> is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>
<p><b>Set command mode port number</b></p>	<p>Sets the TCP command mode port number.</p> <p><b>Important:</b> The optional Flex System Manager software and IBM Director require this port to be 6090.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• 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 287.</li> <li>• You cannot configure a port to a number that is already in use.</li> <li>• Changes to port numbers take effect immediately.</li> <li>• Changing port numbers will affect ongoing operations using the service at that port.</li> </ul>	<p>ports -tcmp <i>TCP_cmd_mdprt_num</i>            where <i>TCP_cmd_mdprt_num</i> is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>

Table 56. ports command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Set secure command mode port number</b></p>	<p>Sets the secure TCP command mode port number.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>You cannot configure a port to a number that is already in use.</li> <li>Changes to port numbers take effect immediately.</li> <li>Changing port numbers will affect ongoing operations using the service at that port.</li> </ul>	<p>ports -stcmp <i>secure_tcmp</i> where <i>secure_tcmp</i> is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>
<p><b>Set SSH port number</b></p>	<p>Sets the port number for the CMM SSH port.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>You cannot configure a port to a number that is already in use.</li> <li>Changes to port numbers take effect immediately.</li> <li>Changing port numbers will affect ongoing operations using the service at that port.</li> </ul>	<p>ports -sshp <i>SSH prt_num</i> where <i>SSH prt_num</i> is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>
<p><b>Set Telnet port number</b></p>	<p>Sets the port number for the CMM Telnet port.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>The Telnet port will not be available if the CMM chassis security level is set to secure with the “security command” on page 287.</li> <li>You cannot configure a port to a number that is already in use.</li> <li>Changes to port numbers take effect immediately.</li> <li>Changing port numbers will affect ongoing operations using the service at that port.</li> </ul>	<p>ports -telnetp <i>Telnet prt_num</i> where <i>Telnet prt_num</i> is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>

Table 56. ports command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Set TFTP port number</b>	<p>Sets the port number for the CMM TFTP port.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>The TFTP port will not be available if the CMM security level is set to secure with the “security command” on page 287.</li> <li>You cannot configure a port to a number that is already in use.</li> <li>Changes to port numbers take effect immediately.</li> <li>Changing port numbers will affect ongoing operations using the service at that port.</li> </ul>	<p>ports -tftp <i>TFTPprt_num</i>            where <i>TFTPprt_num</i> is from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>
<b>Enable / disable FTP</b>	<p>Enables or disables FTP for the CMM.</p> <p><b>Note:</b> The FTP port can not be enabled if the CMM chassis security level is set to secure with the “security command” on page 287.</p>	<p>ports -f tpe <i>state</i>            where <i>state</i> is on or off .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>
<b>Enable / disable SFTP</b>	<p>Enables or disables secure FTP for the CMM.</p>	<p>ports -sftpe <i>state</i>            where <i>state</i> is on or off .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>

Table 56. ports command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Enable / disable HTTPS port</b>	Enables or disables the CMM HTTPS port. <b>Note:</b> Disabling the HTTPS port automatically enables HTTP.	ports -httpse <i>state</i> where <i>state</i> is on or off .  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Enable / disable CIM over HTTPS</b>	Enables or disables CIM over HTTPS for the CMM.	ports -cime <i>state</i> where <i>state</i> is on or off .  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Enable / disable NTP</b>	Enables or disables NTP for the CMM.	ports -ntpe <i>state</i> where <i>state</i> is on or off .  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Enable / disables SLP</b>	Enables or disables SLP for the CMM.	ports -slpe <i>state</i> where <i>state</i> is on or off .  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 56. ports command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Enable / disable SNMPv1 agent</b>	Enables or disables the SNMPv1 agent for the CMM. <b>Note:</b> The SNMPv1 agent can not be enabled if the CMM chassis security level is set to secure with the "security command" on page 287.	ports -snmp1ae <i>state</i> where <i>state</i> is on or off .  This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Enable / disable SNMPv3 agent</b>	Enables or disables the SNMPv3 agent for the CMM.	ports -snmp3ae <i>state</i> where <i>state</i> is on or off .  This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Enable / disable SNMP traps</b>	Enables or disables the SNMP traps for the CMM.	ports -snmpte <i>state</i> where <i>state</i> is on or off .  This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Enable / disable SSH port</b>	Enables or disables the CMM SSH port.	ports -sshe <i>state</i> where <i>state</i> is on or off .  This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See "Commands and user authority" on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 56. ports command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Enable / disable TCP command mode and set number of connections</b></p>	<p>Turns the TCP command mode on or off, or sets the maximum number of connections explicitly.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>Any number of connections (1 through 20) displays a status of on. Zero connections displays a status of off.</li> <li>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 287.</li> <li>The total session count of TCM and STCM is limited to 20.</li> </ul>	<p><code>ports -tcme port_mode</code> where <i>port_mode</i> is on (1 connection), off (no connections), or a number between 0 and 20, inclusive, that indicates the maximum number of TCP session connections.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>
<p><b>Enable / disable secure TCP command mode and set number of connections</b></p>	<p>Turns the secure TCP command mode on or off, or sets the maximum number of connections.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>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).</li> <li>On a read operation, off means 0 connections, and on means 1 or more connections.</li> <li>The total session count of TCM and STCM is limited to 20.</li> </ul>	<p><code>ports -stcme port_mode</code> where <i>port_mode</i> is on (1 connection), off (no connections), or a number between 0 and 20, inclusive, that indicates the maximum number of TCP session connections.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>
<p><b>Enable / disable Telnet port</b></p>	<p>Enables or disables the CMM Telnet port.</p> <p><b>Note:</b> Telnet can not be enabled if the CMM chassis security level is set to secure with the “security command” on page 287.</p>	<p><code>ports -telnet state</code> where <i>state</i> is on or off .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>



Table 56. ports command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Enable / disable TFTP</b></p>	<p>Enables or disables TFTP for the CMM.  <b>Note:</b> TFTP can not be enabled if the CMM security level is set to secure with the “security command” on page 287.</p>	<p>ports - tftpe <i>state</i>            where <i>state</i> is on or off .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>
<p><b>Set FTP timeout</b></p>	<p>Sets the FTP timeout value for the CMM.</p>	<p>ports - fftp <i>timeout</i>            where <i>timeout</i> is from 0 seconds (no timeout) to 4294967295 seconds, inclusive.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>
<p><b>Set TCP command-mode timeout</b></p>	<p>Sets the TCP command-mode timeout value for the CMM.</p>	<p>ports - tcmt <i>timeout</i>            where <i>timeout</i> is from 0 seconds (no timeout) to 4294967295 seconds, inclusive.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>

Table 56. ports command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Set Telnet port timeout</b>	Sets the Telnet port timeout value for the CMM.	<pre>ports -telnet <i>timeout</i></pre> where <i>timeout</i> is from 0 seconds (no timeout) to 4294967295 seconds, inclusive.  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  <pre>mm[p]</pre> <pre>mm[P]</pre> <pre>mm[x]</pre> where <i>x</i> is the primary CMM bay number.
<b>Display network port settings for I/O module</b>	Displays the network port settings for the I/O module. These settings can include: <ul style="list-style-type: none"> <li>• cable compatibility</li> <li>• cable length</li> <li>• cable type</li> <li>• data rate</li> <li>• label</li> <li>• port index</li> <li>• port media</li> <li>• port width</li> <li>• protocol</li> <li>• speed</li> <li>• speed setting</li> <li>• available speeds</li> <li>• state</li> <li>• state setting</li> <li>• type</li> <li>• vendor</li> </ul> <b>Note:</b> Other device specific values might be returned.	<pre>ports</pre>	I/O module:  <pre>switch[x]</pre> where <i>x</i> is the I/O-bay number.

Table 56. ports command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Enable or disable port for I/O module</b>	Enables or disables specified port on specified I/O module.	<p>ports -port_index -state state            where</p> <ul style="list-style-type: none"> <li>• port_index is from 1 to 65535, inclusive.</li> <li>• state is on or off .</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• I/O module configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>I/O module:</p> <p>switch[x]            where x is the I/O-bay number.</p>
<b>Sets speed of port for I/O module</b>	Sets speed of specified port on I/O modules that support this feature.	<p>ports -port_index -speed speed_setting            where</p> <ul style="list-style-type: none"> <li>• port_index is from 1 to 65535, inclusive.</li> <li>• speed_setting specifies the port speed, in terms of:               <ul style="list-style-type: none"> <li>– multiplier</li> <li>– units, m or g for megabits or gigabits</li> <li>– duplex mode, h or f for half or full</li> </ul> </li> </ul> <p>For example:</p> <ul style="list-style-type: none"> <li>– 100mh sets the port speed to 100 Mbps half-duplex.</li> <li>– 10gf sets the port speed to 10 Gbps full-duplex.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• I/O module configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>I/O module:</p> <p>switch[x]            where x is the I/O-bay number.</p>

**Example:**

To display the CMM network port settings, while the Flex System Enterprise 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 Flex System Enterprise 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
-ftp 21
-ftpdp 20
-http 80
-https 443
-slpp 427
-snpap 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
-snmplae 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,
-http, -httpse, -https, -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 385 for a list of error messages that apply to all commands or “power command errors” on page 429 for a list of error messages that are specific to the power command.

Table 57. power command

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Power on</b>	Turns on the specified command target. <b>Note:</b> Some storage nodes might have specific boot sequence requirements, see the documentation for your storage node for details.	<code>power -on</code> This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade administration (for compute node)</li> <li>• I/O module administration (for I/O module)</li> </ul> See "Commands and user authority" on page 10 for additional information.	Compute node:  <code>blade[x]</code> where <i>x</i> is the node bay number.  I/O module:  <code>switch[x]</code> where <i>x</i> is the I/O-bay number.
<b>Power on to command console</b>	Opens a command console with an SOL session when the specified compute node is turned on. <b>Note:</b> Some storage nodes might have specific boot sequence requirements, see the documentation for your storage node for details.	<code>power -on -c</code> This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade administration and blade remote presence</li> </ul> See "Commands and user authority" on page 10 for additional information.	Compute node:  <code>blade[x]</code> where <i>x</i> is the node bay number.
<b>Enable / disable SMS for compute node</b>	Enable or disable the System Management Services (SMS) firmware menu on the specified compute node, for compute nodes that support this feature. <b>Notes:</b> <ul style="list-style-type: none"> <li>• The compute node will restart immediately after setting the <code>-sms</code> option.</li> <li>• The <code>-sms</code> option state that is set is retained after the compute node restarts.</li> <li>• The <code>-sms</code>, <code>-wol</code>, <code>-local</code>, <code>-ap</code>, and <code>-d</code> command options can be entered together, but these options must be used exclusive of all other command options.</li> </ul>	<code>power -sms state</code> where <i>state</i> is enabled or disabled .  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade administration</li> </ul> See "Commands and user authority" on page 10 for additional information.	Compute node:  <code>blade[x]</code> where <i>x</i> is the node bay number.

Table 57. *power* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Power off</b>	Turns off the specified command target.	<p><code>power -off</code></p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade administration (for compute node)</li> <li>• I/O module administration (for I/O module)</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Compute node:</p> <p><code>blade[x]</code> where <i>x</i> is the node bay number.</p> <p>I/O module:</p> <p><code>switch[x]</code> where <i>x</i> is the I/O-bay number.</p>
<b>Shutdown and power off compute node</b>	Shuts down the operating system and turns off the specified compute node.	<p><code>power -softoff</code></p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade administration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Compute node:</p> <p><code>blade[x]</code> where <i>x</i> is the node bay number.</p>
<b>Power cycle</b>	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.	<p><code>power -cycle</code></p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade administration (for compute node)</li> <li>• I/O module administration (for I/O module)</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Compute node:</p> <p><code>blade[x]</code> where <i>x</i> is the node bay number.</p> <p>I/O module:</p> <p><code>switch[x]</code> where <i>x</i> is the I/O-bay number.</p>
<b>Power cycle to command console</b>	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.	<p><code>power -cycle -c</code></p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade administration and blade remote presence</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Compute node:</p> <p><code>blade[x]</code> where <i>x</i> is the node bay number.</p>

Table 57. power command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display power state</b>	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:  blade[x] where x is the node bay number.  I/O module:  switch[x] where x is the I/O-bay number.
<b>Enable / disable Wake on LAN globally</b>	Enables or disables Wake on LAN globally for all compute nodes. <b>Note:</b> 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 where state is enabled or disabled .  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Flex System Enterprise Chassis:  system
<b>Enable / disable Wake on LAN for compute node</b>	Enables or disables Wake on LAN for the specified compute node. <b>Note:</b> 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 where state is enabled or disabled .  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Compute node:  blade[x] where x is the node bay number.
<b>Enable / disable local power control globally</b>	Enables or disables local power control globally for all compute nodes. <b>Note:</b> 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 where state is enabled or disabled .  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Flex System Enterprise Chassis:  system

Table 57. power command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<p><b>Enable / disable local power control for compute node</b></p>	<p>Enables local power control for the specified compute node.  <b>Note:</b> 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.</p>	<p>power -local <i>state</i>            where <i>state</i> is enabled or disabled .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Compute node:</p> <p>blade[x]            where x is the node bay number.</p>
<p><b>Set automatic power-on policy for compute node</b></p>	<p>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.  <b>Note:</b> 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.</p>	<p>power -ap <i>policy</i>            where <i>policy</i> is:</p> <ul style="list-style-type: none"> <li>• restore : the compute node will power on if it was previously on</li> <li>• auto : when power is applied to the Flex System Enterprise Chassis, the compute node will be powered on</li> <li>• manual : the compute node will remain off until manually powered on</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Compute node:</p> <p>blade[x]            where x is the node bay number.</p>



Table 57. power command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<p><b>Set restart delay for compute node</b></p>	<p>Sets the amount of time that the targeted compute node waits to start after application of power to the Flex System Enterprise Chassis. Changes to the restart delay take effect after the next restart of the compute node.</p> <p><b>Note:</b> 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.</p>	<p>power -d <i>value</i>            where <i>value</i> 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.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Compute node:</p> <p>blade[x]            where x is the node bay number.</p>
<p><b>Set restart delay for I/O-module</b></p>	<p>Sets the amount of time that the targeted I/O-module waits to start after application of power to the Flex System Enterprise Chassis. Changes to the restart delay take effect after the next restart of the I/O-module.</p> <p><b>Note:</b> 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.</p>	<p>power -d <i>value</i>            where <i>value</i> 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.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• I/O module administration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>I/O module:</p> <p>switch[x]            where x is the I/O-bay number.</p>
<p><b>Display POST status for I/O module</b></p>	<p>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:</p> <ul style="list-style-type: none"> <li>• The POST results could not be read. message displays if there was an internal error during POST.</li> <li>• The POST results not complete: hex_code message displays if</li> </ul>	<p>power -state -post</p>	<p>I/O module:</p> <p>switch[x]            where x is the I/O-bay number.</p>

Table 57. power command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
	<p>POST results are not available after POST completes.</p> <ul style="list-style-type: none"> <li>• If POST returns valid results, one of the following messages displays: <ul style="list-style-type: none"> <li>– <i>hex_code</i>: Base internal function failure detected.</li> <li>– <i>hex_code</i>: Internal interface failure detected.</li> <li>– <i>hex_code</i>: External interface failure detected.</li> <li>– <i>hex_code</i>: Module completed POST successfully.</li> <li>– <i>hex_code</i>: Cannot decode POST result code.</li> </ul> </li> <li>• The Invalid POST results. message displays if none of the above conditions is true.</li> </ul> <p>Where <i>hex_code</i> is a hexadecimal code. See the documentation that comes with your I/O module for information.</p> <p><b>Note:</b> This command option is not supported for serial concentrator I/O modules.</p>		

**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 385 for a list of error messages that apply to all commands or “pwrprofile command errors” on page 431 for a list of error messages that are specific to the pwrprofile command.

Table 58. *pwrprofile* command

<b>Function</b>	<b>What it does</b>	<b>Command</b>	<b>Target</b> (see paths in “Command targets” on page 6)
<b>Display all power groups and schedules</b>	Displays all power groups and schedules configured for the Flex System Enterprise Chassis.	pwrprofile	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Display power group</b>	Displays information for the specified power group.	pwrprofile -group_index where <i>group_index</i> 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:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 58. *pwrprofile* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Add power group</b></p>	<p>Adds a power group with the specified name for the specified key group of compute nodes and I/O modules.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• All parameters must be specified when creating a power group.</li> <li>• The index number for the power group is assigned automatically and can be seen in the “Display all power groups and schedules” list.</li> </ul>	<p><i>pwrprofile</i> -add -n <i>name</i> -key <i>group_key</i> -servers <i>server_group</i>            where:</p> <ul style="list-style-type: none"> <li>• <i>name</i> 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.</li> <li>• <i>group_key</i> is:               <ul style="list-style-type: none"> <li>– tm for type/model</li> <li>– sn for serial number</li> <li>– by for bay number</li> </ul> </li> <li>• <i>server_group</i> is:               <ul style="list-style-type: none"> <li>– Type/model or serial number (maximum 31 characters). The wildcard character (*) is accepted.</li> <li>– Bay designations that meet the following criteria:                   <ul style="list-style-type: none"> <li>– Maximum string length of 127 characters.</li> <li>– 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.</li> <li>– Bay-type keywords can be in any order separated by a comma.</li> </ul> </li> </ul> </li> </ul> <p><i>(continued on next page)</i></p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>
<p><b>Add power group</b>  <i>(continued)</i></p>		<ul style="list-style-type: none"> <li>• <i>server_group</i>  <i>(continued)</i>:               <ul style="list-style-type: none"> <li>– Bay designations  <i>(continued)</i>:</li> </ul> </li> </ul>	

Table 58. *pwrprofile* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
		<ul style="list-style-type: none"> <li>- Individual bay numbers and ranges can be in any order. Overlapping ranges and whitespace are allowed.</li> </ul> <p>For example:</p> <ul style="list-style-type: none"> <li>- blade (1, 3, 4-6, 8, 2-5, 12, 13-14)</li> <li>- blade (3), blade (5-9, 2)</li> <li>- switch (1-2), blade (1), switch (4)</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> <li>• Chassis log management</li> <li>• Chassis administration</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	
<p><b>Add power schedule and assign to power group</b></p>	<p>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.</p> <p><b>Important:</b> The power group index must be the first command option specified (for example, <code>pwrprofile -1 -add -s enabled -a on -f once -d 11202011</code>).</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• The power group index, <code>-s</code>, <code>-a</code>, and <code>-f</code> parameters must be specified when creating a power schedule.</li> <li>• If the frequency (<code>-f</code>) is set to once, you must specify either a time (<code>-t</code>), a date (<code>-d</code>), 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.</li> <li>• If the frequency (<code>-f</code>) is set to daily, you must specify a time (<code>-t</code>).</li> </ul>	<p><code>pwrprofile -group_index -add -s status -a action -f freq -d day -t time</code>            where:</p> <ul style="list-style-type: none"> <li>• where <code>group_index</code> 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.</li> <li>• <code>status</code> is a power schedule status of enabled or disabled.</li> <li>• <code>action</code> is the power action to perform: <code>on</code>, <code>off</code>, <code>cycle</code>, or <code>softoff</code>.</li> <li>• <code>freq</code> is how often the schedule is applied: <code>once</code>, <code>daily</code>, or <code>weekly</code>.</li> </ul>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where <code>x</code> is the primary CMM bay number.</p>

Table 58. *pwrprofile* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
	<ul style="list-style-type: none"> <li>• If the frequency (-f) is set to weekly, you must specify both a time (-t) and a day (-d).</li> <li>• Up to four power schedules can be assigned to a power group.</li> <li>• The index number for the power schedule is assigned automatically and can be seen in the “Display all power groups and schedules” list.</li> </ul>	<ul style="list-style-type: none"> <li>• <i>day</i> is:               <ul style="list-style-type: none"> <li>– For frequency of once, a date in mmddyyyy format.</li> <li>– For weekly frequency: mon, tues, wed, thur, fri, sat, or sun.</li> </ul> </li> <li>• <i>time</i> is the time of day in hhmm format.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> <li>• Chassis log management</li> <li>• Chassis administration</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	
<p><b>Modify power group</b></p>	<p>Changes values for the specified power group.</p> <p><b>Important:</b> The power group index must be the first command option specified (for example, <code>pwrprofile -1 -n group2</code>).</p> <p><b>Note:</b> You can modify any valid subset of values for the power group.</p>	<p><code>pwrprofile -group_index -n name -key group_key -servers server_group</code>            where:</p> <ul style="list-style-type: none"> <li>• where <i>group_index</i> 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.</li> <li>• <i>name</i> 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.</li> <li>• <i>group_key</i> is:               <ul style="list-style-type: none"> <li>– tm for type/model</li> <li>– sn for serial number</li> <li>– by for bay number</li> </ul> </li> <li>• <i>server_group</i> is:               <ul style="list-style-type: none"> <li>– Type/model or serial number (maximum</li> </ul> </li> </ul>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>

Table 58. pwrprofile command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
		<p>31 characters). The wildcard character (*) is accepted.</p> <ul style="list-style-type: none"> <li>- Bay designations that meet the following criteria:               <ul style="list-style-type: none"> <li>- Maximum string length of 127 characters.</li> <li>- 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.</li> <li>- Bay-type keywords can be in any order separated by a comma.</li> <li>- Individual bay numbers and ranges can be in any order. Overlapping ranges and whitespace are allowed.</li> </ul> </li> </ul> <p>For example:</p> <ul style="list-style-type: none"> <li>• blade (1, 3, 4-6, 8, 2-5, 12, 13-14)</li> <li>• blade (3), blade (5-9, 2)</li> <li>• switch (1-2), blade (1), switch (4)</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> </ul>	

Table 58. *pwrprofile* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
		<ul style="list-style-type: none"> <li>Chassis log management</li> <li>Chassis administration</li> <li>Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	
<b>Modify power schedule</b>	Changes values for the specified power schedule. <b>Notes:</b> <ul style="list-style-type: none"> <li>You can modify any valid subset of values for the power schedule.</li> <li>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.</li> <li>If the frequency (-f) is set to daily, you must specify a time (-t).</li> <li>If the frequency (-f) is set to weekly, you must specify both a time (-t) and a day (-d).</li> </ul>	<pre>pwrprofile -i index -s status -a action -f freq -d day -t time</pre> where: <ul style="list-style-type: none"> <li>where <i>index</i> 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.</li> <li><i>status</i> is a power schedule status of enabled or disabled.</li> <li><i>action</i> is the power action to perform: on, off, cycle, or softoff.</li> <li><i>freq</i> is how often the schedule is applied: once, daily, or weekly.</li> <li><i>day</i> is:               <ul style="list-style-type: none"> <li>For frequency of once, a date in mddyyy format.</li> <li>For weekly frequency: mon, tues, wed, thur, fri, sat, or sun.</li> </ul> </li> <li><i>time</i> is the time of day in hhmm format.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis account management</li> <li>Chassis log management</li> <li>Chassis administration</li> <li>Chassis configuration</li> </ul> See “Commands and user	Primary CMM:  mm[p] mm[P] mm[x] where <i>x</i> is the primary CMM bay number.



Table 58. *pwrprofile* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
		authority” on page 10 for additional information.	
<b>Delete power group</b>	Deletes the specified power group. <b>Important:</b> The power group index must be the first command option specified (for example, <code>pwrprofile -1 -clear</code> ).	<p><code>pwrprofile -group_index -clear</code>            where <i>group_index</i> 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.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> <li>• Chassis log management</li> <li>• Chassis administration</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	Primary CMM:  <code>mm[p]</code> <code>mm[P]</code> <code>mm[x]</code> where <i>x</i> is the primary CMM bay number.

Table 58. *pwrprofile* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Delete power schedule</b>	Deletes the specified power schedule.	<p><code>pwrprofile -clear -i index</code> where <i>index</i> 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.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> <li>• Chassis log management</li> <li>• Chassis administration</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>

**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 2011 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 11202011 -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 11202011 -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 11/20/2011
       -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.

Configurations are saved to a file using the “write command” on page 383.

### 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 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 27.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See “Common errors” on page 385 for a list of error messages that apply to all commands or “read command errors” on page 433 for a list of error messages that are specific to the read command.

Table 59. read command

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<p><b>Restore CMM configuration from file</b></p>	<p>Restores the CMM configuration from an image that was previously saved to a file.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• This image includes CMM users and permission groups.</li> <li>• Password information stored in the configuration file is encrypted.</li> <li>• Users must have permission to modify any settings controlled by individual commands in the configuration being restored.</li> </ul>	<p>read -u <i>URL</i> -p <i>passphrase</i>            where:</p> <ul style="list-style-type: none"> <li>• <i>URL</i> is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the configuration file is located.</li> <li>• "<i>passphrase</i>" 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.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>
<p><b>Restore CMM configuration from file (verbose)</b></p>	<p>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.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• This image includes CMM users and permission groups.</li> <li>• Password information stored in the configuration file is encrypted.</li> <li>• Users must have permission to modify any settings controlled by individual commands in the configuration being restored.</li> </ul>	<p>read -u <i>URL</i> -p <i>passphrase</i> -v            where:</p> <ul style="list-style-type: none"> <li>• <i>URL</i> is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the configuration file is located.</li> <li>• "<i>passphrase</i>" 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.</li> </ul>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>

Table 59. read command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
		<p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	
<p><b>Restore CMM configuration from file and reset CMM</b></p>	<p>Restores the CMM configuration from an image that was previously saved to a file and then reset the CMM.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• This image includes CMM users and permission groups.</li> <li>• Password information stored in the configuration file is encrypted.</li> <li>• The CMM resets in all cases, even if restoring the configuration fails.</li> <li>• Users must have permission to modify any settings controlled by individual commands in the configuration being restored.</li> </ul>	<p>read -u <i>URL</i> -p <i>passphrase</i> -r</p> <p>where:</p> <ul style="list-style-type: none"> <li>• <i>URL</i> is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the configuration file is located.</li> <li>• "<i>passphrase</i>" 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.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>

Table 59. read command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<p><b>Restore CMM configuration from file (verbose) and reset CMM</b></p>	<p>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.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• This image includes CMM users and permission groups.</li> <li>• Password information stored in the configuration file is encrypted.</li> <li>• The CMM resets in all cases, even if restoring the configuration fails.</li> <li>• Users must have permission to modify any settings controlled by individual commands in the configuration being restored.</li> </ul>	<p><code>read -u URL -p passphrase -v -r</code>            where:</p> <ul style="list-style-type: none"> <li>• <i>URL</i> is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the configuration file is located.</li> <li>• "<i>passphrase</i>" 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.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>

**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 Flex System Enterprise 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>
```

**remotechassis command**

This command displays and manages the list of each Flex System Enterprise 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 385 for a list of error messages that apply to all commands or “remotechassis command errors” on page 434 for a list of error messages that are specific to the remotechassis command.

Table 60. remotechassis command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display complete list</b>	Displays a list of all Flex System Enterprise Chassis that the CMM discovers on the network. The list includes the following information about each Flex System Enterprise Chassis: <ul style="list-style-type: none"> <li>• Name</li> <li>• IP address</li> <li>• Status</li> <li>• Firmware level</li> <li>• Type</li> <li>• Serial number</li> <li>• FRU number</li> <li>• Chassis serial number</li> <li>• Chassis FRU number</li> <li>• Chassis machine-type model (MTM)</li> <li>• Chassis UUID</li> </ul>	remotechassis	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Display list grouped by health status</b>	Displays a list of names for Flex System Enterprise Chassis that the CMM discovers on the network. The list is grouped by health status.	remotechassis -health	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Display list filtered by IP address</b>	Displays a list of Flex System Enterprise Chassis that the CMM discovers on the network, filtered by the specified IP address. The list includes the following information about each Flex System Enterprise Chassis: <ul style="list-style-type: none"> <li>• Name</li> <li>• IP address</li> <li>• Status</li> <li>• Firmware level</li> <li>• Type</li> <li>• Serial number</li> <li>• FRU number</li> <li>• Chassis serial number</li> <li>• Chassis FRU number</li> <li>• Chassis machine-type model (MTM)</li> <li>• Chassis UUID</li> </ul>	remotechassis -ip <i>ip_address</i> where <i>ip_address</i> is an IP address pattern that uses the asterisk (*) as a wildcard (for example; 201.47.123.*).	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.



Table 60. `remotechassis` command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Display list filtered by name</b>	<p>Displays a list of Flex System Enterprise Chassis that the CMM discovers on the network, filtered by the specified name. The list includes the following information about each Flex System Enterprise Chassis:</p> <ul style="list-style-type: none"> <li>• Name</li> <li>• IP address</li> <li>• Status</li> <li>• Firmware level</li> <li>• Type</li> <li>• Serial number</li> <li>• FRU number</li> <li>• Chassis serial number</li> <li>• Chassis FRU number</li> <li>• Chassis machine-type model (MTM)</li> <li>• Chassis UUID</li> </ul>	<p><code>remotechassis -name <i>name</i></code>            where <i>name</i> is a name pattern that uses the asterisk (*) as a wildcard (for example; <code>WebServer*</code>).</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where x is the primary CMM bay number.</p>
<b>Clear list</b>	<p>Clears the list of Flex System Enterprise Chassis that the CMM discovered on the network.</p>	<p><code>remotechassis -clear</code></p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where x is the primary CMM bay number.</p>

**Example:**

To list all Flex System Enterprise 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 Flex System Enterprise 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 385 for a list of error messages that apply to all commands or “reset command errors” on page 435 for a list of error messages that are specific to the reset command.

Table 61. reset command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Reset</b>	Performs an immediate reset and restart of the specified device.	<code>reset</code> This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"><li>• Supervisor</li><li>• Blade administration (for compute node or compute node ISMP)</li><li>• I/O module administration (for I/O module)</li></ul> See “Commands and user authority” on page 10 for additional information.	Compute node:  <code>blade[x]</code> where <i>x</i> is the node bay number.  Compute node system-management processor:  <code>sp</code>  I/O module:  <code>switch[x]</code> where <i>x</i> is the I/O-bay number.
<b>Reset primary CMM</b>	Performs an immediate reset and restart of the primary CMM. If the current operating state of the Flex System Enterprise Chassis indicates potential problems with performing the reset, an error message is returned and the reset is cancelled.	<code>reset</code> This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"><li>• Supervisor</li><li>• Chassis administration</li></ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  <code>mm[p]</code> <code>mm[P]</code> <code>mm[x]</code> where <i>x</i> is the primary CMM bay number.
<b>Reset primary CMM (with override)</b>	Performs an immediate reset and restart of the primary CMM, overriding error messages and reset cancellation due to the current Flex System Enterprise Chassis operating state.	<code>reset -o</code> This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"><li>• Supervisor</li><li>• Chassis administration</li></ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  <code>mm[p]</code> <code>mm[P]</code> <code>mm[x]</code> where <i>x</i> is the primary CMM bay number.

Table 61. reset command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Reset standby CMM</b>	Performs an immediate reset of the standby CMM.	reset -standby This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis administration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.  <b>Note:</b> Even though this command resets the standby CMM, it still must specify the primary CMM as the command target.
<b>Reset compute node to command console</b>	Opens a command console with an SOL session when the specified compute node is reset.	reset -c This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade administration and blade remote presence</li> </ul> See “Commands and user authority” on page 10 for additional information.	Compute node:  blade[x] where x is the node bay number.
<b>Reset with failover</b>	Resets the specified command target, enabling failover if a redundant (standby) component for the command target is present. 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 This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis administration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Reset I/O module with standard diagnostics</b>	Performs an immediate reset and restart of the specified device, running standard diagnostics on the I/O module after it restarts. Running the <b>reset -std</b> command gives the same result as running the <b>reset</b> command on a I/O module.	reset -std This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• I/O module administration</li> </ul> See “Commands and user authority” on page 10 for additional information.	I/O module:  switch[x] where x is the I/O-bay number.

Table 61. reset command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Reset I/O module with extended diagnostics</b>	Performs an immediate reset and restart of the specified device, running extended diagnostics on the I/O module after it restarts.	reset -exd This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• I/O module administration</li> </ul> See “Commands and user authority” on page 10 for additional information.	I/O module:  switch[x] where x is the I/O-bay number.
<b>Reset I/O module with full diagnostics</b>	Performs an immediate reset and restart of the specified device, running full diagnostics on the I/O module after it restarts.	reset -full This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• I/O module administration</li> </ul> See “Commands and user authority” on page 10 for additional information.	I/O module:  switch[x] where x is the I/O-bay number.
<b>Restart compute node with NMI</b>	Performs an immediate reset and restart of the specified compute node, for compute nodes that support the non-maskable interrupt (NMI). <b>Note:</b> A compute node must be powered on to run the reset -sft command.	reset -sft This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade administration and blade remote presence</li> </ul> See “Commands and user authority” on page 10 for additional information.	Compute node:  blade[x] where x is the node bay number.

**Example:** To reset the system-management processor on the compute node in node bay 5, while the Flex System Enterprise 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 Flex System Enterprise 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 385 for a list of error messages that apply to all commands or “scale command errors” on page 437 for a list of error messages that are specific to the scale command.

Table 62. scale command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display all scalable complex information</b>	Displays all scalable complex information for the Flex System Enterprise Chassis.	scale	Flex System Enterprise Chassis:  system
<b>Display information for specific scalable complex</b>	Displays information for the specified scalable complex. <b>Notes:</b> <ul style="list-style-type: none"> <li>• The <i>complex_id</i> is found by running the scale command with no options.</li> <li>• The -c <i>compid</i> command option is required for only compute node systems that can have multiple scalable complexes defined in the same Flex System Enterprise Chassis. This option does not need to be specified for stand-alone systems.</li> </ul>	scale -c <i>compid</i> <i>complex_id</i> where <i>complex_id</i> is a unique complex identifier (hexadecimal string of four alphanumeric characters), assigned by the compute node complex.	Flex System Enterprise Chassis:  system

Table 62. *scale* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display information for specific node in a scalable complex</b>	Displays information for a specific node in the scalable complex. <b>Notes:</b> <ul style="list-style-type: none"> <li>The <i>complex_id</i> and <i>node_id</i> are found by running the <i>scale</i> command with no options.</li> <li>The <i>-compid</i> command option is required for only compute node systems that can have multiple scalable complexes defined in the same Flex System Enterprise Chassis. This option does not need to be specified for stand-alone systems.</li> </ul>	<i>scale -compid complex_id -node node_id</i> where : <ul style="list-style-type: none"> <li><i>complex_id</i> is a unique complex identifier (hexadecimal string of four alphanumeric characters), assigned by the compute node complex.</li> <li><i>node_id</i> is the compute node bay number, of the node.</li> </ul>	Flex System Enterprise Chassis:  system
<b>Display information for specific partition in a scalable complex</b>	Displays information for a specific partition in the scalable complex. <b>Notes:</b> <ul style="list-style-type: none"> <li>The <i>complex_id</i> and <i>partition_id</i> are found by running the <i>scale</i> command with no options.</li> <li>The <i>-compid</i> command option is required for only compute node systems that can have multiple scalable complexes defined in the same Flex System Enterprise Chassis. This option does not need to be specified for stand-alone systems.</li> </ul>	<i>scale -compid complex_id -partid partition_id</i> where : <ul style="list-style-type: none"> <li><i>complex_id</i> is a unique complex identifier (hexadecimal string of four alphanumeric characters), assigned by the compute node complex.</li> <li><i>partition_id</i> is a partition identifier, assigned by the compute node complex.</li> </ul>	Flex System Enterprise Chassis:  system

**Example:** To view all scalable complexes in the system, while the Flex System Enterprise 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 Flex System Enterprise 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 Flex System Enterprise 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 Flex System Enterprise 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: NANW00R  
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 385 for a list of error messages that apply to all commands or “sddump command errors” on page 437 for a list of error messages that are specific to the sddump command.

Table 63. *sddump* command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Dump service data (compute node)</b>	<p>Dumps service data of the specified type from the specified compute node target.</p> <ul style="list-style-type: none"> <li>For compute nodes with an IMM, data dumps are initiated and collected from the CMM.</li> <li>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.</li> </ul>	<p><code>sddump -init type</code> where <i>type</i> is:</p> <ul style="list-style-type: none"> <li><code>sd</code> for a service data dump.</li> <li><code>sp</code> for a node system-management processor data dump.</li> <li><code>pf</code> for a platform data dump.</li> <li><code>pt</code> for a partition data dump.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Blade administration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Compute node:</p> <p><code>blade[x]</code> where <i>x</i> is the node bay number.</p>
<b>Dump service data (I/O module)</b>	<p>Dumps service data from the specified I/O-module target.</p> <p><b>Note:</b> To successfully obtain a data dump from an I/O module, the I/O module must support data collection.</p>	<p><code>sddump -init</code></p>	<p>I/O module:</p> <p><code>switch[x]</code> where <i>x</i> is the I/O-bay number.</p>
<b>Get service data</b>	<p>Collects service data, from the last generated service-data dump, of the specified type from the specified compute node target.</p>	<p><code>sddump -coll type</code> where <i>type</i> is:</p> <ul style="list-style-type: none"> <li><code>sd</code> to collect service data from last dump.</li> <li><code>sp</code> to collect node system-management processor data from last dump.</li> <li><code>pf</code> to collect platform data from last dump.</li> <li><code>pt</code> to collect partition data from last dump.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Blade administration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Compute node:</p> <p><code>blade[x]</code> where <i>x</i> is the node bay number.</p>

**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:blade2 >` prompt, type `sddump -init sp`

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

```
system:blade[2]> sddump -init sp
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 385 for a list of error messages that apply to all commands or “sdemail command errors” on page 438 for a list of error messages that are specific to the sdemail command.

Table 64. *sdemail* command

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<p><b>Send service information using email to specified recipients</b></p>	<p>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.</p>	<p><code>sdemail -subj "subject" -to address</code>            where:</p> <ul style="list-style-type: none"> <li>• "subject" is a quote-delimited text string up to 119 characters in length.</li> <li>• address is the recipients email address. Multiple addresses separated with a comma can be entered (119 characters maximum).</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> <li>• Chassis log management</li> <li>• Chassis administration</li> <li>• Chassis configuration</li> <li>• Blade administration</li> <li>• Blade configuration</li> <li>• Blade remote presence</li> <li>• I/O module administration</li> <li>• I/O module configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>

**Example:**

To send a service information email message, while the Flex System Enterprise Chassis is set as the persistent command environment, at the `system >` prompt, type `sdemail -T mm[p] -to mail@cn.ibm.com -subj "Blade 8 Reboot"`

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

```
system> sdemail -T mm[p] -to mail@cn.ibm.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 385 for a list of error messages that apply to all commands or “security command errors” on page 438 for a list of error messages that are specific to the security command.

Table 65. security command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display CMM chassis security policy</b>	<p>Displays the chassis security policy information for the CMM:</p> <ul style="list-style-type: none"> <li>• Security policy level (legacy or secure).</li> <li>• Security policy state: <ul style="list-style-type: none"> <li>– Active indicates that the security policy is in force.</li> <li>– Pending indicates that the changes are needed, such as disabling non-secure protocols, before the policy can become active.</li> </ul> </li> <li>• Version of the security policy rule definitions being enforced.</li> </ul>	security	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>
<b>Set CMM chassis security policy level</b>	<p>Sets the chassis security policy level for the CMM.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• To set the chassis security policy level to secure, “accseccfg command” on page 35 options must be set as follows: <ul style="list-style-type: none"> <li>– -cp (complex password): on</li> <li>– -de (default account password change at next login): on</li> <li>– -pc (password change on first access): on</li> </ul> </li> <li>• The following interfaces must be disabled, using the “ports command” on page 240, before setting the CMM chassis security level to secure: <ul style="list-style-type: none"> <li>– HTTP</li> <li>– FTP</li> <li>– SNMPv1</li> <li>– Telnet</li> <li>– TFTP</li> <li>– Non-secure TCP command mode</li> </ul> </li> </ul>	<p>security -p <i>level</i> where <i>level</i> is legacy or secure .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>

**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 385 for a list of error messages that apply to all commands or “service command errors” on page 438 for a list of error messages that are specific to the service command.

**Attention:** If you are managing your Flex System chassis using the optional Flex System Manager software, you must unmanage and remanage the chassis when performing virtual reseal (service-level reset) of the primary CMM using the `service -vr` command. See [http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.8731.doc/product\\_page.html](http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.8731.doc/product_page.html) for more information.



Table 66. service command

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<p><b>Virtual reset</b></p>	<p>Performs a virtual reset (service-level reset) of the specified command target. A virtual reset simulates physical removal and insertion of the command target. The virtual reset removes standby power from the command target and then restores it. Each command target type has unique behavior when virtually reset:</p> <ul style="list-style-type: none"> <li>• A CMM or I/O module is automatically powered on after the virtual reset.</li> <li>• A compute node or storage node remains off after a virtual reset and the user will need to power it back on. The command forcibly shuts down the compute node operating system.</li> <li>• 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.</li> </ul> <p><b>Attention:</b></p> <ul style="list-style-type: none"> <li>• Performing a virtual reset on Flex System components might result in the loss of data. Do not perform a virtual reset unless you are instructed by Lenovo Support. Prior to executing a virtual reset, perform any needed operations to protect user data.</li> <li>• Performing a virtual reset on an Flex System V7000 storage node (or storage cluster) might result in the loss of data. Do not perform a virtual reset on an Flex System V7000 storage node (or storage cluster) unless you are instructed by Lenovo Support. Prior to executing a virtual reset, perform any needed operations to protect user data.</li> </ul> <p><b>Important:</b></p> <ul style="list-style-type: none"> <li>• Instead of performing a virtual reset on an Flex System V7000 storage node, use the "Powering on and powering off the clustered system" procedure to power off an Flex System V7000 storage node, if needed (see <a href="#">"Powering on and powering off the clustered system" in the Flex System V7000 Storage Node library</a>).</li> </ul> <p><i>(continued on next page)</i></p>	<p>service -vr</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• For the CMM target: <ul style="list-style-type: none"> <li>– Supervisor</li> <li>– Chassis Administration</li> <li>– Chassis Configuration</li> </ul> </li> <li>• For the compute node or storage node target: <ul style="list-style-type: none"> <li>– Supervisor</li> <li>– Blade Administration</li> <li>– Blade Configuration</li> </ul> </li> <li>• For the I/O Module target: <ul style="list-style-type: none"> <li>– Supervisor</li> <li>– I/O Module Administration</li> </ul> </li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary or standby CMM:</p> <p>mm[p] mm[P] mm[s] mm[S] mm[x] where x is the primary or standby CMM bay number.</p> <p>Compute node or storage node:</p> <p>blade[x] where x is the node bay number.</p> <p>I/O module:</p> <p>switch[x] where x is the I/O-bay number.</p>
<p><b>Virtual reset</b> <i>(continued)</i></p>	<ul style="list-style-type: none"> <li>• If you do perform a virtual reset on an 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 reset option (see <a href="#">"Troubleshooting" in the Flex System V7000 Storage Node library</a>).For</li> </ul>		

Table 66. service command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
	<p>more information on Flex System V7000 storage node error 578, see "<a href="#">Error 578</a>" in the <a href="#">Flex System V7000 Storage Node library</a>.</p> <ul style="list-style-type: none"> <li>• During a virtual reseal, the component will experience a temporary loss of communication and its power state will change.</li> <li>• If you are managing your Flex System chassis using the optional Flex System Manager software, you must unmanage and remanage the chassis when performing virtual reseal (service-level reset) of the primary CMM. See <a href="http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.8731.doc/product_page.html">http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.8731.doc/product_page.html</a> for information.</li> </ul> <p><b>Note:</b> Do not perform a virtual reseal 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 applications such as the optional Flex System Manager software.</p>		
<p><b>Virtual reseal of primary CMM (suppress warnings for standby CMM)</b></p>	<p>Performs a virtual reseal (service-level reset) of the specified command target. A virtual reseal simulates physical removal and insertion of the command target. The virtual reseal removes standby power from the command target and then restores it.</p> <ul style="list-style-type: none"> <li>• A CMM is automatically powered on after the virtual reseal.</li> <li>• The -o command option suppresses warnings about the standby CMM state.</li> </ul> <p><b>Attention:</b></p> <ul style="list-style-type: none"> <li>• During a virtual reseal, you will temporarily lose communication with the command target and its power state will change. Before performing a virtual reseal, make sure that you perform any actions necessary to protect user data.</li> <li>• If you are managing your Flex System chassis using the optional Flex System Manager software, you must unmanage and remanage the chassis when performing virtual reseal (service-level reset) of the primary CMM. See <a href="http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/chassis_unmanage.html">http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/chassis_unmanage.html</a> and "<a href="#">Remanaging a chassis after unmanaging</a>" for information.</li> </ul>	<p><code>service -vr -o</code></p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis Administration</li> <li>• Chassis Configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary or standby CMM:</p> <p>mm[p] mm[P] mm[s] mm[S] mm[x] where x is the primary or standby CMM bay number.</p>

Table 66. *service* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Hard restart</b>	<p>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.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Not all compute nodes support the hard restart function.</li> <li>• A system-management processor does not need to be responsive in order to reset it.</li> </ul>	<p><code>service -hard</code></p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Blade Administration</li> <li>• Blade Configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Compute node system-management processor:</p> <p>sp</p>

**Example:**

To perform a virtual reset (service-level reset) of the I/O module in bay 1, while the Flex System Enterprise Chassis is set as the persistent command environment, at the `system >` prompt, type

```
service -T switch[1] -vr
```

To perform a hardware reset of the compute node (service processor) in bay 1, while the Flex System Enterprise Chassis is set as the persistent command environment, at the `system >` prompt, type

```
service -T blade[1]:sp -hard
```

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 385 for a list of error messages that apply to all commands or “smtp command errors” on page 439 for a list of error messages that are specific to the smtp command.

Table 67. *smtp* command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display SMTP server host name or IP address</b>	Displays the SMTP server domain name and host name or IP address.	<code>smtp</code>	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Server host name or IP address - set</b>	Checks syntax and sets the server host name or IP address.	<code>smtp -s hostname/ip_address</code> where <i>hostname/ip_address</i> 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 (“”).  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>SMTP e-mail server domain name - set</b>	Checks syntax and sets the SMTP e-mail server domain name.	<code>smtp -d domainname</code> where <i>domainname</i> is a valid domain name that meets the following criteria: <ul style="list-style-type: none"> <li>• Alphanumeric string up to 63 characters in length.</li> <li>• Can contain dots (.), dashes (-), or underscores (_).</li> <li>• Must contain at least one dot.</li> <li>• No consecutive dots are allowed.</li> <li>• Quotes are not required.</li> <li>• Value can be cleared by setting it to an empty, double-quote delimited string (“”).</li> </ul> This command can only be run by users who have	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 67. 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: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	

**Example:**

To set the SMTP server host name to us.ibm.com, while the primary CMM in bay 1 is set as the persistent command environment, at the `system: mm[1] >` prompt, type  
`smtp -s us.ibm.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 us.ibm.com
OK
system:mm[1]> smtp
-s us.ibm.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 385 for a list of error messages that apply to all commands or “snmp command errors” on page 440 for a list of error messages that are specific to the snmp command.

Table 68. snmp command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display SNMP configuration of CMM</b>	Displays the current SNMP configuration of the CMM.	snmp	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>SNMPv1 agent - enable/disable</b>	Enables or disables the CMM SNMPv1 agent. <b>Notes:</b> <ul style="list-style-type: none"> <li>Before you can enable the SNMPv1 agent, the following must be specified (see “config command” on page 95): <ul style="list-style-type: none"> <li>CMM contact name</li> <li>CMM location</li> <li>at least one community name</li> <li>at least one valid IP address for that community</li> </ul> </li> <li>SNMPv1 can not be enabled if the CMM chassis security level is set to secure with the “security command” on page 287.</li> </ul>	snmp -a -state where state is on or off .  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>SNMPv3 agent - enable/disable</b>	Enables or disables the CMM SNMPv3 agent. <b>Notes:</b> Before you can enable the SNMPv3 agent, the following must be specified: <ul style="list-style-type: none"> <li>CMM contact name</li> <li>CMM location</li> </ul> (see “config command” on page 95)	snmp -a3 -state where state is on or off .  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>SNMP traps - enable/disable</b>	Enables or disables the CMM SNMP traps. <b>Note:</b> SNMPv1 ports will not be available if the CMM chassis security level is set to secure with the “security command” on page 287.	snmp -t -state where state is on or off .  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 68. snmp command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>SNMP community 1 name - set</b>	Sets the name of community 1.	<pre>snmp -c1 name</pre> <p>where <i>name</i> is a descriptive name of community 1.</p> <ul style="list-style-type: none"> <li>Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments.</li> <li>If this argument is not specified, the snmp command clears this option.</li> <li>You can also clear this option by assigning an empty string as its value.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	Primary CMM:  mm[p] mm[P] mm[x] where <i>x</i> is the primary CMM bay number.
<b>SNMP community 1 first host name or IP address - set</b>	Checks syntax and sets the first host name or IP address of community 1.	<pre>snmp -cli1 hostname/ip_address</pre> <p>where <i>hostname/ip_address</i> is the first host name or IP address of community 1.</p> <ul style="list-style-type: none"> <li>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.</li> <li>Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments.</li> <li>If this argument is not specified, the snmp command clears this option.</li> <li>You can also clear this option by assigning an empty string as its value.</li> </ul> <p>This command can only be run by users who have one</p>	Primary CMM:  mm[p] mm[P] mm[x] where <i>x</i> is the primary CMM bay number.

Table 68. snmp command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
		or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	
<b>SNMP Community 1, first host name - set access to SET (wildcard)</b>	Sets the access type for community 1 to SET.	<pre>snmp -cal set -c1i1 0.0.0.0</pre> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments.</li> <li>• If this argument is not specified, the snmp command clears this option.</li> <li>• You can also clear this option by assigning an empty string as its value.</li> </ul> This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM: mm[p] mm[P] mm[x] where x is the primary CMM bay number.



Table 68. snmp command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>SNMP Community 1, first host name or IP address - set access to GET (wildcard)</b></p>	<p>Sets the access type for community 1 to GET.</p>	<p><code>snmp -ca1 get -c1i1 0.0.0.0</code></p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments.</li> <li>• If this argument is not specified, the snmp command clears this option.</li> <li>• You can also clear this option by assigning an empty string as its value.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>
<p><b>SNMP community 1 second host name or IP address - set</b></p>	<p>Checks syntax and sets the second host name or IP address of community 1.</p>	<p><code>snmp -c1i2 hostname/ip_ address</code> where <i>hostname/ip_ address</i> is the second host name or IP address of community 1.</p> <ul style="list-style-type: none"> <li>• Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments.</li> <li>• If this argument is not specified, the snmp command clears this option.</li> <li>• You can also clear this option by assigning an empty string as its value.</li> </ul> <p>This command can only be run by users who have one</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>

Table 68. snmp command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
		or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	
<b>SNMP community 1 third host name or IP address - set</b>	Checks syntax and sets the third host name or IP address of community 1.	<pre>snmp -c1i3 hostname/ip_address</pre> where <i>hostname/ip_address</i> is the third host name or IP address of community 1. <ul style="list-style-type: none"> <li>• Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments.</li> <li>• If this argument is not specified, the snmp command clears this option.</li> <li>• You can also clear this option by assigning an empty string as its value.</li> </ul> This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM: mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>SNMPv3 community 1 view type - set</b>	Sets the SNMPv3 view type for community 1.	<pre>snmp -ca1 type</pre> where <i>type</i> is <ul style="list-style-type: none"> <li>• get</li> <li>• set</li> <li>• trap</li> </ul> This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM: mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 68. snmp command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>SNMP community 2 name - set</b>	Sets the name of community 2.	<pre>snmp -c2 name</pre> <p>where <i>name</i> is a descriptive name of community 2.</p> <ul style="list-style-type: none"> <li>Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments.</li> <li>If this argument is not specified, the snmp command clears this option.</li> <li>You can also clear this option by assigning an empty string as its value.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	Primary CMM:  mm[p] mm[P] mm[x] where <i>x</i> is the primary CMM bay number.
<b>SNMP community 2 first host name or IP address - set</b>	Checks syntax and sets the first host name or IP address of community 2.	<pre>snmp -c2i1 hostname/ip_address</pre> <p>where <i>hostname/ip_address</i> is the first host name or IP address of community 2.</p> <ul style="list-style-type: none"> <li>Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments.</li> <li>If this argument is not specified, the snmp command clears this option.</li> <li>You can also clear this option by assigning an empty string as its value.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	Primary CMM:  mm[p] mm[P] mm[x] where <i>x</i> is the primary CMM bay number.

Table 68. snmp command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
		additional information.	
<b>SNMP community 2 second host name or IP address - set</b>	Checks syntax and sets the second host name or IP address of community 2.	<p>snmp -c2i2 <i>hostname/ip_address</i>            where <i>hostname/ip_address</i> is the second host name or IP address of community 2.</p> <ul style="list-style-type: none"> <li>Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments.</li> <li>If this argument is not specified, the snmp command clears this option.</li> <li>You can also clear this option by assigning an empty string as its value.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 68. snmp command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>SNMP community 2 third host name or IP address - set</b>	Checks syntax and sets the third host name or IP address of community 2.	<pre>snmp -c 2i3 hostname/ip_ address</pre> where <i>hostname/ip_</i> <i>address</i> is the third host name or IP address of community 2. <ul style="list-style-type: none"> <li>• Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments.</li> <li>• If this argument is not specified, the snmp command clears this option.</li> <li>• You can also clear this option by assigning an empty string as its value.</li> </ul> This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>SNMPv3 community 2 view type - set</b>	Sets the SNMPv3 view type for community 2.	<pre>snmp -ca2 type</pre> where <i>type</i> is <ul style="list-style-type: none"> <li>• get</li> <li>• set</li> <li>• trap</li> </ul> This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 68. snmp command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>SNMP community 3 name - set</b>	Sets the name of community 3.	<pre>snmp -c3 name</pre> where <i>name</i> is a descriptive name of community 3. <ul style="list-style-type: none"> <li>Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments.</li> <li>If this argument is not specified, the snmp command clears this option.</li> <li>You can also clear this option by assigning an empty string as its value.</li> </ul> This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM: mm[p] mm[P] mm[x] where <i>x</i> is the primary CMM bay number.
<b>SNMP community 3 first host name or IP address - set</b>	Checks syntax and sets the first host name or IP address of community 3.	<pre>snmp -c3i1 hostname/ip_address</pre> where <i>hostname/ip_address</i> is the first host name or IP address of community 3. <ul style="list-style-type: none"> <li>Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments.</li> <li>If this argument is not specified, the snmp command clears this option.</li> <li>You can also clear this option by assigning an empty string as its value.</li> </ul> This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for	Primary CMM: mm[p] mm[P] mm[x] where <i>x</i> is the primary CMM bay number.

Table 68. snmp command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
		additional information.	
<b>SNMP community 3 second host name or IP address - set</b>	Checks syntax and sets the second host name or IP address of community 3.	<pre>snmp -c 3i2 hostname/ip_ address</pre> <p>where <i>hostname/ip_</i> address is the second host name or IP address of community 3.</p> <ul style="list-style-type: none"> <li>Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments.</li> <li>If this argument is not specified, the snmp command clears this option.</li> <li>You can also clear this option by assigning an empty string as its value.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	Primary CMM:  mm[p] mm[P] mm[x] where <i>x</i> is the primary CMM bay number.

Table 68. snmp command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>SNMP community 3 third host name or IP address - set</b>	Checks syntax and sets the third host name or IP address of community 3.	<p>snmp -c3i3 <i>hostname/ip_address</i></p> <p>where <i>hostname/ip_address</i> is the third host name or IP address of community 3.</p> <ul style="list-style-type: none"> <li>Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments.</li> <li>If this argument is not specified, the snmp command clears this option.</li> <li>You can also clear this option by assigning an empty string as its value.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where <i>x</i> is the primary CMM bay number.</p>
<b>SNMPv3 community 3 view type - set</b>	Sets the SNMPv3 view type for community 3.	<p>snmp -ca3 <i>type</i></p> <p>where <i>type</i> is</p> <ul style="list-style-type: none"> <li>get</li> <li>set</li> <li>trap</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where <i>x</i> is the primary CMM bay number.</p>



Table 68. snmp command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>SNMP contact name - set</b>	Sets the contact name.	<p>snmp -cn <i>contact_name</i>            where <i>contact_name</i> is the name of the party to be contacted when SNMP traps an event.</p> <ul style="list-style-type: none"> <li>Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments.</li> <li>If this argument is not specified, the snmp command clears this option.</li> <li>You can also clear this option by assigning an empty string as its value.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>SNMP location - set</b>	Sets the location.	<p>snmp -l <i>hostname/ip_address</i>            where <i>hostname/ip_address</i> identifies the website supporting SNMP for this CMM.</p> <ul style="list-style-type: none"> <li>Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments.</li> <li>If this argument is not specified, the snmp command clears this option.</li> <li>You can also clear this option by assigning an empty string as its value.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user</p>	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 68. 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 26). 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 385 for a list of error messages that apply to all commands or “sol command errors” on page 440 for a list of error messages that are specific to the sol command.

Table 69. sol command

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<p><b>Display SOL status</b></p>	<p>Displays the SOL status for the targeted device:</p> <ul style="list-style-type: none"> <li>• When the command target is the primary CMM, it displays the following values: <ul style="list-style-type: none"> <li>– -status <i>on/off</i> (global SOL status)</li> <li>– -c <i>retry_count</i></li> <li>– -e <i>CLI_key_sequence</i></li> <li>– -i <i>retry_interval</i></li> <li>– -r <i>reset_blade_key_seq</i></li> <li>– -s <i>send_threshold</i></li> <li>– -t <i>accumulate_timeout</i></li> </ul> </li> <li>• When the command target is a compute node, it displays the following: <ul style="list-style-type: none"> <li>– -status <i>enabled/disabled</i> (SOL status for the compute node)</li> <li>– Status of any SOL sessions for that compute node: <ul style="list-style-type: none"> <li>– Not ready</li> <li>– Ready</li> <li>– Active</li> </ul> </li> <li>– SOL retry interval</li> <li>– SOL retry count</li> <li>– SOL bytes sent</li> <li>– SOL bytes received</li> <li>– SOL destination IP address (IPv6 format)</li> <li>– SOL destination MAC address</li> <li>– SOL console user ID</li> <li>– SOL console login IP address</li> <li>– SOL console session start time</li> <li>– SOL console session stop time</li> <li>– Compute node power state</li> </ul> </li> </ul>	<p>sol</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p> <p>Compute node:</p> <p>blade[x] where x is the node bay number.</p>
<p><b>SOL retry interval - set</b></p>	<p>Sets the SOL retry interval to the input value.</p>	<p>sol -i <i>value</i> where <i>value</i> 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.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>

Table 69. sol command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
		<ul style="list-style-type: none"> <li>Blade configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	
<b>SOL retry count - set</b>	Sets the SOL retry count to the input value.	sol -c <i>value</i> where <i>value</i> 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.  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> <li>Blade configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>SOL send threshold - set</b>	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 <i>value</i> where <i>value</i> is from 1 to 251, inclusive. If you enter a value outside this range, an error will be displayed.  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> <li>Blade configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 69. sol command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>SOL accumulate timeout - set</b>	Sets the SOL accumulate timeout to the input value.	<p>sol -t <i>value</i>            where <i>value</i> 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.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> <li>• Blade configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>
<b>SOL enable - global</b>	Enables SOL globally for the Flex System Enterprise Chassis. The global SOL enable command does not affect the SOL session status for each compute node.	<p>sol -status enabled            This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> <li>• Blade configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>
<b>SOL enable - compute node</b>	Enables SOL for the specified compute node.	<p>sol -status enabled            This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> <li>• Blade configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Compute node:</p> <p>blade[x]            where x is the node bay number.</p>

Table 69. sol command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>SOL disable - global</b>	Disables SOL globally for the Flex System Enterprise Chassis. The global SOL disable command does not affect the SOL session status for each compute node.	sol -status disabled This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> <li>• Blade configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>SOL disable - compute node</b>	Disables SOL for the specified compute node.	sol -status disabled This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> <li>• Blade configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	Compute node:  blade[x] where x is the node bay number.

Table 69. sol command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>CLI key sequence - set</b></p>	<p>Sets the key sequence that is used to enter the CLI while a Telnet session in SOL mode.</p>	<p>sol -e <i>value</i>            where <i>value</i> is the key sequence. In this sequence, a ^ (the carat symbol) indicates a Ctrl that maps to control-key sequences; for example:</p> <ul style="list-style-type: none"> <li>• ^[ (the carat symbol followed by a left bracket) means Esc</li> <li>• ^M (the carat symbol followed by a capitol M) means carriage return.</li> </ul> <p>Refer to an ASCII-to-key conversion table for a complete listing of control-key sequences.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> <li>• Blade configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>
<p><b>Reset compute node key sequence - set</b></p>	<p>Sets the key sequence that will reset a compute node while a Telnet session in SOL mode.</p>	<p>sol -r <i>value</i>            where <i>value</i> is the key sequence. In this sequence, a ^ (the carat symbol) indicates a Ctrl that maps to control-key sequences; for example:</p> <ul style="list-style-type: none"> <li>• ^[ (the carat symbol followed by a left bracket) means Esc</li> <li>• ^M (the carat symbol followed by a capitol M) means carriage return.</li> </ul> <p>Refer to an ASCII-to-key conversion table for a complete listing of control-key sequences.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> </ul>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>

Table 69. sol command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
		<ul style="list-style-type: none"> <li>• Chassis configuration</li> <li>• Blade configuration</li> </ul> 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
SQL Session: Ready
SQL retry interval: 64000 ms
SQL retry count: 7
SQL bytes sent: 0
SQL bytes received: 0
SQL destination IP address: FE80::3BA7:94FF:FE07:CBDD
SQL destination MAC: unknown
SQL console user ID:
SQL console login from:
```



```

SQL console session started:
SQL 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 385 for a list of error messages that apply to all commands or “sshcfg command errors” on page 442 for a list of error messages that are specific to the sshcfg command.

Table 70. sshcfg command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display SSH status</b>	Displays the SSH status of the CMM. Returned values are: <ul style="list-style-type: none"> <li>• -cstatus: state of CLI SSH server (enabled, disabled)</li> <li>• -sftpstatus: state of secure FTP server (enabled, disabled)</li> <li>• CLI SSH port number</li> <li>• ssh-dss fingerprint</li> <li>• ssh-rsa fingerprint</li> <li>• number of SSH public keys installed</li> <li>• number of locations available to store SSH keys</li> </ul> <b>Note:</b> For scripting purposes, the “-v1 off” state is always displayed.	sshcfg	Primary CMM: mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Display RSA host key information</b>	Displays RSA host key information for the CMM.	sshcfg -hk rsa	Primary CMM: mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Display DSA host key information</b>	Displays DSA host key information for the CMM.	sshcfg -hk dsa	Primary CMM: mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 70. sshcfg command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Generate host key</b>	Generates a host key for the CMM.	sshcfg -hk gen This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Set state of CLI SSH server</b>	Sets the state of the CLI SSH server for the CMM.	sshcfg -cstatus <i>state</i> where <i>state</i> is enabled or disabled .  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Set state of CLI SFTP server</b>	Sets the state of the CLI secure FTP (SFTP) server for the CMM.	sshcfg -sftpstatus <i>state</i> where <i>state</i> is enabled or disabled .  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] 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. Insecure 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”. Insecure 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 27.
- SHA256 certificates are not supported for external LDAP servers.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See “Common errors” on page 385 for a list of error messages that apply to all commands or “sslcfg command errors” on page 442 for a list of error messages that are specific to the sslcfg command.

Table 71. sslcfg command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display CMM SSL status</b>	Displays the SSL status of the specified CMM. This status includes information about SSL certificates.	sslcfg	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Set SSL (secure LDAP) state for LDAP client</b>	Enables or disables SSL (secure LDAP) for the LDAP client. <b>Notes:</b> <ul style="list-style-type: none"> <li>• By default, the LDAP client uses the same SSL certificate as the LDAP server.</li> <li>• The LDAP client can be enabled if a certificate is in place.</li> </ul>	sslcfg -client <i>state</i> where <i>state</i> is enabled or disabled .  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 71. `sslcfg` command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Set SSL state for HTTPS server</b>	Enables or disables the HTTPS server. <b>Note:</b> The HTTPS server can be enabled if a certificate is in place.	<code>sslcfg -server state</code> where <i>state</i> is enabled or disabled .  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  <code>mm[p]</code> <code>mm[P]</code> <code>mm[x]</code> where <i>x</i> is the primary CMM bay number.
<b>View self-signed certificate</b>	Views a certificate authority self-signed root certificate for the CMM.	<code>sslcfg -view ca</code>	Primary CMM:  <code>mm[p]</code> <code>mm[P]</code> <code>mm[x]</code> where <i>x</i> is the primary CMM bay number.

Table 71. `sslcfg` command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<p><b>Generate self-signed certificate</b></p>	<p>Generates a self-signed certificate for the chassis certificate authority.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>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.</li> <li>If the <code>crypto -m</code> option is set to <code>comp</code>, for compatibility with all NIST cipher suites (see the "crypto command" on page 103 for more information), the <code>sslcfg -gen ca -csa certificate type</code> option must be specified when generating a CA certificate.</li> <li>If the <code>crypto -m</code> option is set to <code>nist800-131a</code> (see the "crypto command" on page 103 for more information), the <code>sslcfg -gen ca -csa</code> option is optional; if it is specified, the certificate type must be set to <code>rsa2048sha256</code>.</li> </ul>	<p><code>sslcfg -gen ca -csa type</code> where the optional certificate type is:</p> <ul style="list-style-type: none"> <li><code>rsa2048sha1</code></li> <li><code>rsa2048sha256</code></li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where x is the primary CMM bay number.</p>
<p><b>Generate CSR</b></p>	<p>Generates a certificate signing request (CSR) for the CMM HTTPS server or LDAP client. The following values must be set when generating a CSR:</p> <ul style="list-style-type: none"> <li>Country using the <code>-c</code> command option.</li> <li>State or province using the <code>-sp</code> command option.</li> <li>City or locality using the <code>-cl</code> command option.</li> <li>Organization name using the <code>-on</code> command option.</li> <li>CMM host name using the <code>-hn</code> command option.</li> </ul>	<p><code>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</code> where the following required options are:</p> <ul style="list-style-type: none"> <li><code>country</code> is two-character alphabetic code for the country.</li> </ul>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where x is the primary CMM bay number.</p>

Table 71. *sslcfg* command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
	<p><b>Note:</b> This host name must match the host name that is used by a web browser to connect to the CMM.</p> <p>The following optional values can be set when generating a CSR:</p> <ul style="list-style-type: none"> <li>• Contact person using the <b>-cp</b> command option.</li> <li>• Email address of the contact person using the <b>-ea</b> command option.</li> <li>• Unit within a company or organization using the <b>-ou</b> command option.</li> <li>• Additional information such as a surname using the <b>-s</b> command option.</li> <li>• Additional information such as a given name using the <b>-gn</b> command option.</li> <li>• Additional information such as a initials using the <b>-in</b> command option.</li> <li>• Additional information such as a distinguished name qualifier using the <b>-dq</b> command option.</li> <li>• Additional information such as a CSR password using the <b>-cpwd</b> command option.</li> <li>• Additional information such as an unstructured name qualifier using the <b>-un</b> command option.</li> </ul>	<ul style="list-style-type: none"> <li>• "state" is a state or province name of up to 60 characters in length.</li> <li>• "city" is a city or locality name of up to 50 characters in length.</li> <li>• "org" is an organization name of up to 60 characters in length.</li> <li>• <i>hostname</i> is a valid host name of up to 60 characters in length.</li> <li>• <i>target</i> is server or client</li> </ul> <p>where the following optional options are:</p> <ul style="list-style-type: none"> <li>• "name" is up to 60 characters in length.</li> <li>• <i>email</i> is a valid email address of up to 60 characters.</li> <li>• "org_unit" is up to 60 characters.</li> <li>• "surname" is up to 60 characters.</li> </ul> <p>(continued on next page)</p>	
<p><b>Generate CSR</b> (continued)</p>		<ul style="list-style-type: none"> <li>• "given_name" is up to 60 characters.</li> <li>• "initial" is up to 20 characters.</li> <li>• "dn_qualifier" is up to 60 characters.</li> <li>• <i>password</i> is between 6 and 30 characters.</li> <li>• "un_name" is up to 60 characters.</li> </ul> <p><b>Note:</b> Arguments that must be quote-delimited are shown in quotation marks.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user</p>	

Table 71. `sslcfg` command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
		authority” on page 10 for additional information.	
<p><b>Download CA self-signed root certificate file</b></p>	<p>Downloads the specified CA self-signed root certificate file. 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 <code>-u</code> command option.</p> <p><b>Note:</b> To successfully download and import a CA certificate into an external LDAP server trust store, make sure that secure LDAP is enabled using the <code>sslcfg -server</code> enabled or the <code>sslcfg -client</code> enabled command.</p>	<p><code>sslcfg -dnld ca -u URL</code> where <i>URL</i> is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the certificate file is located.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where <i>x</i> is the primary CMM bay number.</p>

Table 71. `sslcfg` command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Download certificate or CSR file of specified format</b></p>	<p>Downloads the specified certificate file, specifying the certificate file format.</p> <p>The location of the certificate or CSR file, including IP address of the server for downloading and filename, and must be set using the <code>-u</code> command option.</p> <p><b>Note:</b> If the certificate or CSR file format is not specified using the <code>-f</code> command option, the format defaults to DER.</p>	<p><code>sslcfg -dnld cert_type -f format -u URL -t target</code>            where:</p> <ul style="list-style-type: none"> <li>• <code>cert_type</code> is               <ul style="list-style-type: none"> <li>– <code>cert</code> for a certificate</li> <li>– <code>csr</code> for a CSR (for the CMM LDAP client certificate)</li> </ul> </li> <li>• <code>format</code> is               <ul style="list-style-type: none"> <li>– <code>der</code> for binary DER encoded certificates</li> <li>– <code>pem</code> for X.509v3 files that contain ASCII (Base64) armored data prefixed with a BEGIN line</li> </ul> </li> <li>• <code>URL</code> is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the certificate file is located.</li> <li>• <code>target</code> is server or client</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>
<p><b>Import (upload) trusted certificate 1</b></p>	<p>Import (upload) trusted certificate 1 for the LDAP client.</p> <p>The upload location of the trusted certificate file, including IP address of the server and filename, an must be set using the <code>-u</code> command option.</p>	<p><code>sslcfg -tc1 import -u URL -t client</code>            where <code>URL</code> is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the certificate file is located.</p> <p><b>Note:</b> The <code>-t client</code> option is optional. If it is not specified, the command defaults to the client target.</p> <p>This command can only be run by users who have one or more of the</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>



Table 71. `sslcfg` command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
		following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	
<b>Import (upload) trusted certificate 2</b>	Import (upload) trusted certificate 2 for the LDAP client. The upload location of the trusted certificate file, including IP address of the server and filename, must be set using the <code>-u</code> command option.	<pre>sslcfg -tc2 import -u URL -t client</pre> where <i>URL</i> is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the certificate file is located. <p><b>Note:</b> The <code>-t client</code> option is optional. If it is not specified, the command defaults to the client target.</p> This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM: mm[p] mm[P] mm[x] where <i>x</i> is the primary CMM bay number.

Table 71. `sslcfg` command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Import (upload) trusted certificate 3</b></p>	<p>Import (upload) trusted certificate 3 for the LDAP client.</p> <p>The upload location of the trusted certificate file, including IP address of the server and filename, must be set using the <code>-u</code> command option.</p>	<p><code>sslcfg -tc3 import -u URL -t client</code>            where <i>URL</i> is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the certificate file is located.</p> <p><b>Note:</b> The <code>-t client</code> option is optional. If it is not specified, the command defaults to the client target.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where <i>x</i> is the primary CMM bay number.</p>
<p><b>Export (download) trusted certificate 1</b></p>	<p>Downloads (exports) trusted certificate 1 for the LDAP client.</p> <p>The location of the trusted certificate 1 file, including IP address of the server for downloading and filename, must be set using the <code>-u</code> command option.</p>	<p><code>sslcfg -tc1 download -u URL -t client</code>            where <i>URL</i> is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the certificate file is located.</p> <p><b>Note:</b> The <code>-t client</code> option is optional. If it is not specified, the command defaults to the client target.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where <i>x</i> is the primary CMM bay number.</p>

Table 71. *sslcfg* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Export (download) trusted certificate 2</b></p>	<p>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.</p>	<p><code>sslcfg -tc2 download -u URL -t client</code>            where <i>URL</i> is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the certificate file is located.  <b>Note:</b> The -t client option is optional. If it is not specified, the command defaults to the client target.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>
<p><b>Export (download) trusted certificate 3</b></p>	<p>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.</p>	<p><code>sslcfg -tc3 download -u URL -t client</code>            where <i>URL</i> is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the certificate file is located.  <b>Note:</b> The -t client option is optional. If it is not specified, the command defaults to the client target.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>

Table 71. `sslcfg` command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Remove trusted certificate 1</b>	Removes trusted certificate 1 from the LDAP client.	<code>sslcfg -tc1 remove -t client</code> <b>Note:</b> The <code>-t client</code> option is optional. If it is not specified, the command defaults to the client target. This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  <code>mm[p]</code> <code>mm[P]</code> <code>mm[x]</code> where <code>x</code> is the primary CMM bay number.
<b>Remove trusted certificate 2</b>	Removes trusted certificate 2 from the LDAP client.	<code>sslcfg -tc2 remove -t client</code> <b>Note:</b> The <code>-t client</code> option is optional. If it is not specified, the command defaults to the client target. This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  <code>mm[p]</code> <code>mm[P]</code> <code>mm[x]</code> where <code>x</code> is the primary CMM bay number.

Table 71. `sslcfg` command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Remove trusted certificate 3</b>	Removes trusted certificate 3 from the LDAP client.	<pre>sslcfg -tc3 remove -t client</pre> <p><b>Note:</b> The <code>-t client</code> option is optional. If it is not specified, the command defaults to the client target. This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	Primary CMM:  <code>mm[p]</code> <code>mm[P]</code> <code>mm[x]</code> where <code>x</code> is the primary CMM bay number.
<b>Import (upload) certificate</b>	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 <code>-u</code> command option.	<pre>sslcfg -upld -u URL -t target</pre> <p>where:</p> <ul style="list-style-type: none"> <li>• <code>URL</code> is fully qualified uniform resource locator, including file name, of the <code>tftp</code>, <code>ftp</code>, <code>http</code>, <code>https</code>, or <code>sftp</code> server where the certificate file is located.</li> <li>• <code>target</code> is server or client</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	Primary CMM:  <code>mm[p]</code> <code>mm[P]</code> <code>mm[x]</code> where <code>x</code> 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: mm1 >` 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: mm1 >` 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 enabled
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: Available
  Trusted Certificate 2: Not available
  Trusted Certificate 3: Not available
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 385 for a list of error messages that apply to all commands or “syslog command errors” on page 444 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 72. *syslog* command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display syslog configuration</b>	Displays the syslog event log transmission configuration of the CMM.	syslog	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Set syslog filter level</b>	Set severity filtering levels for syslog event log transmission.	syslog -sev <i>level</i> where <i>level</i> is: <ul style="list-style-type: none"> <li>• i selects error, warning, and informational logs</li> <li>• w selects error and warning logs</li> <li>• e selects error logs</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> <li>• Chassis log management</li> <li>• Chassis administration</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Set syslog event log transmission state for collector 1</b>	Enables or disables syslog event log transmission to collector 1.	syslog -coll1 <i>state</i> where <i>state</i> is enabled or disabled .  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> <li>• Chassis log management</li> <li>• Chassis administration</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 72. *syslog* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Set syslog event log transmission state for collector 2</b></p>	<p>Enables or disables syslog event log transmission to collector 2.</p>	<p><code>syslog -coll2 state</code>            where <i>state</i> is enabled or disabled .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> <li>• Chassis log management</li> <li>• Chassis administration</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where <i>x</i> is the primary CMM bay number.</p>
<p><b>Syslog event log collector 1 host name or IP address - set</b></p>	<p>Sets the host name or IP address for syslog event collector 1.</p>	<p><code>syslog -i1 hostname/ip_address</code>            where <i>hostname/ip_address</i> is the collector 1 host name or IP address.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> <li>• Chassis log management</li> <li>• Chassis administration</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where <i>x</i> is the primary CMM bay number.</p>



Table 72. *syslog* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Syslog event log collector 2 host name or IP address - set</b>	Sets the host name or IP address for syslog event collector 2.	<pre>syslog -i2 hostname/ip_ address</pre> where <i>hostname/ip_</i> <i>address</i> is the collector 2 host name or IP address. <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> <li>• Chassis log management</li> <li>• Chassis administration</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM: <pre>mm[p] mm[P] mm[x]</pre> where <i>x</i> is the primary CMM bay number.
<b>Syslog event log collector 1 port number - set</b>	Sets the port number for syslog event collector 1.	<pre>syslog -p1 port</pre> where <i>port</i> is the collector 1 port number from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed. <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> <li>• Chassis log management</li> <li>• Chassis administration</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM: <pre>mm[p] mm[P] mm[x]</pre> where <i>x</i> is the primary CMM bay number.

Table 72. *syslog* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Syslog event log collector 2 port number - set</b>	Sets the port number for syslog event collector 2.	<p><code>syslog -p2 port</code>                      where <i>port</i> is the collector 2 port number from 1 to 65535, inclusive. If you enter a value outside this range, an error will be displayed.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> <li>• Chassis log management</li> <li>• Chassis administration</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Generate test message</b>	Generates a test syslog message to test the configuration. <b>Note:</b> The -test command options must be run exclusive of other command options.	<p><code>syslog -test</code>                      This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> <li>• Chassis log management</li> <li>• Chassis administration</li> <li>• Chassis configuration</li> <li>• Blade administration</li> <li>• Blade configuration</li> <li>• Blade remote presence</li> <li>• I/O module administration</li> <li>• I/O module configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
Set timestamp format	Set timestamp format for syslog event log transmission.	<p><code>syslog -f format</code>                      where <i>format</i> is:</p> <ul style="list-style-type: none"> <li>• default</li> </ul> <p>where the timestamp format is like in this example</p> <p>‘Thu Mar 1</p>	Primary CMM:  -T system:mm[x] .  where x is the primary management-module bay number.

Table 72. syslog command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
		<pre>07:42:53 2018'</pre> <ul style="list-style-type: none"> <li>• RFC3164</li> </ul> <p>where the timestamp format is compliant with RFC 3164. Example: 'Mar 1 07:42:53'</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	

**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 the optional 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 385 for a list of error messages that apply to all commands or “tcpcmdmode command errors” on page 445 for a list of error messages that are specific to the tcpcmdmode command.

Table 73. *tcpcmdmode* command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display TCP command-mode session status and timeout</b>	Displays the secure and non-secure TCP command-mode session status (maximum number of sessions) and timeout.	<code>tcpcmdmode</code>	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Set TCP command-mode session timeout</b>	Sets the secure and non-secure TCP command-mode session timeout value.	<code>tcpcmdmode -t timeout</code> where <i>timeout</i> is from 0 seconds (no timeout) to 4294967295 seconds, inclusive. If you enter a value outside this range, an error will be displayed.  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Disable TCP command-mode sessions</b>	Disables TCP command-mode sessions that are used by the optional Flex System Manager software for out-of-band communication with the CMM. This applies to both read and write operations.	<code>tcpcmdmode -status 0</code> This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 73. *tcpcmdmode* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Enable and set number of TCP command-mode sessions</b></p>	<p>Enables TCP command-mode and sets the maximum number of sessions that can be used by the optional Flex System Manager software for out-of-band communication with the CMM. For read operations, all of the values from 1 to 20, inclusive, mean <i>enabled</i>.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>The CMM supports a combined total of up to 20 secure and non-secure TCP command-mode sessions.</li> <li>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 287.</li> </ul>	<p><code>tcpcmdmode -status <i>number_sessions</i></code>            where <i>number_sessions</i> 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.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where x is the primary CMM bay number.</p>
<p><b>Disable secure TCP command-mode sessions</b></p>	<p>Disables secure TCP command-mode sessions that are used by the optional Flex System Manager software for out-of-band communication with the CMM. This applies to both read and write operations.</p>	<p><code>tcpcmdmode -sstatus 0</code>            This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where x is the primary CMM bay number.</p>
<p><b>Enable and set number of secure TCP command-mode sessions</b></p>	<p>Enables secure TCP command-mode and sets the maximum number of sessions that can be used by optional Flex System Manager software for out-of-band communication with the CMM. For read operations, all of the values from 1 to 20, inclusive, mean <i>enabled</i>.</p> <p><b>Note:</b> The CMM supports a combined total of up to 20 secure and non-secure TCP command-mode sessions.</p>	<p><code>tcpcmdmode -sstatus <i>number_sessions</i></code>            where <i>number_sessions</i> 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.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where x is the primary CMM bay number.</p>

**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 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 385 for a list of error messages that apply to all commands or “temps command errors” on page 446 for a list of error messages that are specific to the temps command.

Table 74. temps command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display temperature values</b>	Displays the current temperature and temperature threshold settings for the specified component: <ul style="list-style-type: none"> <li>The compute node target displays the temperature values for components in the specified compute node, such as microprocessors and expansion modules.</li> <li>The rear LED card target displays values for the temperature sensor in the rear LED card.</li> </ul>	temps	Compute node: blade[x] where x is the node bay number.  Rear LED card: 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 Flex System Enterprise 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]

```

Component	Value	Warning	Hard Shutdown	Warning 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 385 for a list of error messages that apply to all commands or “trespass command errors” on page 446 for a list of error messages that are specific to the trespass command.

Table 75. *trespass* command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display status of CMM trespass feature</b>	Displays status of the trespass feature for the CMM. Possible return values are: <ul style="list-style-type: none"> <li>-twe (on or off)</li> <li>-tw <i>warning_message</i></li> </ul> <b>Note:</b> The <i>warning_message</i> is shown only when the trespass feature is enabled (-twe on).	trespass	Primary CMM: mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Enable / disable CMM trespass feature</b>	Enables or disables trespass feature for CMM.	trespass -twe <i>state</i> where <i>state</i> is on or off .  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM: mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 75. trespass command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<p><b>Set CMM trespass message</b></p>	<p>Sets message that is displayed to users who log in to the CMM when the trespass feature is enabled.  <b>Note:</b> Setting a new <i>warning_message</i> permanently replaces the default warning message.</p>	<p><code>trespass -tw "warning_message"</code>            where <i>warning_message</i> is up to 1600 characters in length and enclosed in double-quotation marks.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>
<p><b>Set CMM trespass feature to default values</b></p>	<p>Sets trespass feature to default values:</p> <ul style="list-style-type: none"> <li>• -twe: off</li> <li>• -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</li> </ul>	<p><code>trespass -twd</code>            This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>



Table 75. 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 385 for a list of error messages that apply to all commands or "uicfg command errors" on page 446 for a list of error messages that are specific to the uicfg command.

Table 76. uicfg command

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Display CMM user interface settings</b>	Displays the user interface settings for the CMM. Returned values indicate enabled or disabled status for the following interfaces: <ul style="list-style-type: none"> <li>• -cim (common information model used by the optional Flex System Manager software)</li> <li>• -cli (command line)</li> <li>• -snmp</li> <li>• -tcm (TCP command mode)</li> <li>• -stcm (secure TCP command mode)</li> <li>• -web (web interface)</li> </ul>	uicfg	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Enable / disable command-line interface</b>	Enables or disables the CMM command-line interface (using Telnet or SSH). <b>Note:</b> The Telnet interface will not be available if the CMM chassis security level is set to secure with the "security command" on page 287.	uicfg -cli <i>state</i> where <i>state</i> is enabled or disabled .  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Enable / disable CIM</b>	Enables or disables the CMM common information model (CIM) interface used by the optional Flex System Manager software.	uicfg -cim <i>state</i> where <i>state</i> is enabled or disabled .  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 76. uicfg command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Enable / disable SNMPv1 and SNMPv3</b></p>	<p>Enables or disables SNMPv1 and SNMPv3 connections to the CMM.  <b>Note:</b> SNMPv1 connections will not be available if the CMM chassis security level is set to secure with the “security command” on page 287.</p>	<p><code>uicfg -snmp state</code>            where <i>state</i> is enabled or disabled .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where <i>x</i> is the primary CMM bay number.</p>
<p><b>Disable or set number of TCP command mode connections</b></p>	<p>Disable the TCP command mode (used by the optional Flex System Manager software) for the CMM, or explicitly set the maximum number of TCP command mode connections.  <b>Notes:</b></p> <ul style="list-style-type: none"> <li>• Any number of connections (1 through 20) displays a status of enabled. Zero connections displays a status of disabled.</li> <li>• 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 287.</li> </ul>	<p><code>uicfg -tcm port_mode</code>            where <i>port_mode</i> is:</p> <ul style="list-style-type: none"> <li>• disabled (no connections)</li> <li>• enabled (1 connection)</li> <li>• a number between 0 and 20, inclusive, that indicates the maximum number of non-secure TCP session connections</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where <i>x</i> is the primary CMM bay number.</p>

Table 76. uicfg command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Disable or set number of secure TCP command mode connections</b>	<p>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.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>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).</li> <li>On a read operation, disabled means 0 connections, and enabled means 1 or more connections.</li> <li>The total session count of TCM and STCM is limited to 20.</li> </ul>	<p>uicfg -stcm <i>port_mode</i>            where <i>port_mode</i> is:</p> <ul style="list-style-type: none"> <li>disabled (no connections)</li> <li>enabled (1 connection)</li> <li>a number between 0 and 20, inclusive, that indicates the maximum number of secure TCP session connections</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>
<b>Enable / disable web interface</b>	<p>Enables or disables the CMM web interface.</p>	<p>uicfg -web <i>state</i>            where <i>state</i> is enabled or disabled .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>

**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 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 27.
- The CMM update command does not support updating compute node firmware. If an optional Flex System Manager management server is installed in the Flex System Enterprise Chassis, you can update compute node firmware using the Flex System Manager 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 Flex System, see the *Firmware Update Best Practices Guide* at <https://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 385 for a list of error messages that apply to all commands or “update command errors” on page 447 for a list of error messages that are specific to the update command.

Table 77. update command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Display firmware attributes</b></p>	<p>Displays attributes of the firmware installed in the command target. Return values are:</p> <ul style="list-style-type: none"> <li>• Firmware type</li> <li>• Build ID</li> <li>• Filename</li> <li>• Release date</li> <li>• Revision level</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• For a standby CMM, the returned value will also indicate if a firmware update is in progress and the percentage that is complete.</li> <li>• For I/O modules that support it, this command will also display firmware image information.</li> </ul>	<p>update -a</p>	<p>Primary or standby CMM:</p> <p>mm[p] mm[P] mm[s] mm[S] mm[x] where x is the primary or standby CMM bay number.</p> <p>I/O module:</p> <p>switch[x] where x is the I/O-bay number.</p>
<p><b>Update firmware using URL</b></p>	<p>Update firmware for the command target using a uniform resource locator (URL).</p> <p><b>Attention:</b></p> <ul style="list-style-type: none"> <li>• Installing the wrong firmware update might cause the CMM to malfunction.</li> </ul> <p><b>Important:</b> 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).</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• Updating to older firmware levels may cause loss of certain functionality.</li> <li>• 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.</li> <li>• Some I/O modules support only RSA fingerprinting when updating through SFTP. See the</li> </ul>	<p>update -u <i>URL</i> where <i>URL</i> 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.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis administration (for CMM)</li> <li>• I/O module administration (for I/O module)</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p> <p>I/O module:</p> <p>switch[x] where x is the I/O-bay number.</p>

Table 77. 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.		
<b>Update firmware and reboot</b>	<p>Update firmware and reboot the CMM to use new firmware if the update succeeds.</p> <p><b>Attention:</b></p> <ul style="list-style-type: none"> <li>Installing the wrong firmware update might cause the CMM to malfunction.</li> </ul> <p><b>Important:</b> 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.</p> <p><b>Note:</b> 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.</p>	<p>update -u <i>URL</i> -r            where <i>URL</i> 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.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis administration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where <i>x</i> is the primary CMM bay number.</p>

Table 77. update command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Update firmware (verbose)</b></p>	<p>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.</p> <p><b>Attention:</b></p> <ul style="list-style-type: none"> <li>Installing the wrong firmware update might cause the CMM to malfunction.</li> </ul> <p><b>Important:</b> 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.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>Updating to older firmware levels may cause loss of certain functionality.</li> <li>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.</li> <li>Some I/O modules support only RSA fingerprinting when updating through SFTP. See the documentation that comes with your I/O module for information.</li> </ul>	<p>update -u <i>URL</i> -v where <i>URL</i> 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.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis administration (for CMM)</li> <li>I/O module administration (for I/O module)</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p> <p>I/O module:</p> <p>switch[x] where x is the I/O-bay number.</p>
<p><b>Update I/O module firmware</b></p>	<p>Directly update I/O module firmware image.</p> <p><b>Attention:</b> 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.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>Only some I/O modules have this capability.</li> </ul>	<p>update -u <i>URL</i> -img <i>img_index</i> where:</p> <ul style="list-style-type: none"> <li><i>URL</i> 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.</li> <li><i>img_index</i> is the image index you are updating. Use the update -a command to list available images and their index numbers.</li> </ul>	<p>I/O module:</p> <p>switch[x] where x is the I/O-bay number.</p>



Table 77. update command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
	<ul style="list-style-type: none"> <li>Some I/O modules support only RSA fingerprinting when updating through SFTP. See the documentation that comes with your I/O module for information.</li> </ul>	<p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>I/O module administration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	
<p><b>Update I/O module firmware (verbose)</b></p>	<p>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.</p> <p><b>Attention:</b> 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.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>Only some I/O modules have this capability.</li> <li>Some I/O modules support only RSA fingerprinting when updating through SFTP. See the documentation that comes with your I/O module for information.</li> </ul>	<p><code>update -u URL -img img_index -v</code>            where:</p> <ul style="list-style-type: none"> <li><code>URL</code> 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.</li> <li><code>img_index</code> is the image index to the I/O module firmware you are updating. Use the <code>update -a</code> command to list available images and their index numbers.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>I/O module administration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>I/O module:</p> <p><code>switch[x]</code>            where <code>x</code> is the I/O-bay number.</p>

Table 77. update command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Activate I/O module firmware</b></p>	<p>Directly activate I/O module firmware image.</p> <p><b>Note:</b> Only some I/O modules have this capability.</p>	<p>update - activate <i>img_index</i>            where <i>img_index</i> is the image index you are activating. Use the update -a command to list available images and their index numbers.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• I/O module administration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>I/O module:</p> <p>switch[x]            where x is the I/O-bay number.</p>
<p><b>Update and activate I/O module firmware</b></p>	<p>Directly update I/O module and activate the firmware image.</p> <p><b>Attention:</b> 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.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• Only some I/O modules have this capability.</li> <li>• The activate option can be used with the other options. You can flash first, then activate the specified index.</li> <li>• The image index you activate can be different from the one you update.</li> <li>• Some I/O modules support only RSA fingerprinting when updating through SFTP. See the documentation that comes with your I/O module for information.</li> </ul>	<p>update -u <i>URL</i> -img <i>img_index</i> - activate <i>img_index</i>            where:</p> <ul style="list-style-type: none"> <li>• <i>URL</i> 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.</li> <li>• <i>img_index</i> is the image index you are activating. Use the update -a command to list available images and their index numbers.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• I/O module administration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>I/O module:</p> <p>switch[x]            where x is the I/O-bay number.</p>



that the chassis is operating properly before replacing either CMM. See [Troubleshooting chassis](#) for information about diagnosing problems with a Flex System Enterprise 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 385 for a list of error messages that apply to all commands or “uplink command errors” on page 451 for a list of error messages that are specific to the uplink command.

Table 78. *uplink command*

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display uplink failover status</b>	Displays the CMM uplink failover status (enabled or disabled) and the failover delay.	uplink	Flex System Enterprise Chassis: system  Primary CMM: mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Set physical network uplink failover delay</b>	Sets the amount of time between detection of a CMM physical uplink failure and failover to the standby CMM.	uplink -dps <i>delay</i> where <i>delay</i> is from 10 to 172800 seconds, inclusive. If you enter a value outside this range, an error will be displayed.  This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See “Commands and user authority” on page 10 for additional information.	Flex System Enterprise Chassis: system  Primary CMM: mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Enable / disable physical uplink failover</b>	Enables or disables failover to the standby CMM if the external physical network interface of the primary CMM fails.	uplink -ep <i>state</i> where <i>state</i> is enabled or disabled .  This command can only be run by users who have one or more of the following command authorities: • Supervisor • Chassis configuration See “Commands and user authority” on page 10 for additional information.	Flex System Enterprise Chassis: system  Primary CMM: mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 78. uplink command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Set logical network uplink failover delay</b></p>	<p>Sets the amount of time between detection of a CMM logical uplink failure and failover to the standby CMM.</p>	<p>uplink -dls <i>delay</i>            where <i>delay</i> is from 60 to 172800 seconds, inclusive. If you enter a value outside this range, an error will be displayed.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Flex System Enterprise Chassis:</p> <p style="padding-left: 40px;">system</p> <p>Primary CMM:</p> <p style="padding-left: 40px;">mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>
<p><b>Enable / disable logical uplink failover</b></p>	<p>Enables or disables failover to the standby CMM if the external logical network interface of the primary CMM fails.</p> <p>Failure is indicated when all of the following conditions occur:</p> <ul style="list-style-type: none"> <li>• Loss of CMM eth0 input and output packets</li> <li>• Network noise</li> <li>• Failures when pinging the CMM gateway and a designated station</li> </ul> <p>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.</p>	<p>uplink -el <i>state</i>            where <i>state</i> is enabled or disabled .</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Flex System Enterprise Chassis:</p> <p style="padding-left: 40px;">system</p> <p>Primary CMM:</p> <p style="padding-left: 40px;">mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>

Table 78. uplink command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Set IP address to check logical network uplink</b>	Sets the IPv4 IP address of the device that the CMM accesses to check its logical network link.	uplink -ip <i>ip_address</i> where <i>ip_address</i> 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.  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Flex System Enterprise Chassis:  system  Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Set IPv6 IP address to check logical network uplink</b>	Sets the IPv6 IP address of the device that the CMM accesses to check its logical network link.	uplink -ip6 <i>ip_address</i> where <i>ip_address</i> is a valid, non-zero, IPv6 IP address. You must enter a non-zero IPv6 IP address before you can enable logical uplink failover.  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Flex System Enterprise Chassis:  system  Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Set logical link loss alert and failover policy</b>	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. <b>Notes:</b> The -alert command option applies only when: <ul style="list-style-type: none"> <li>• Both the -ip and -ip6 command options are set.</li> <li>• Both IP addresses are non-zero.</li> <li>• IPv6 is enabled using the ifconfig command.</li> </ul>	uplink -alert <i>setting</i> where <i>setting</i> is: <ul style="list-style-type: none"> <li>• either to check either the IPv4 IP address or the IPv6 IP address.</li> <li>• both to check both the IPv4 IP address and the IPv6 IP address.</li> </ul> This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul>	Flex System Enterprise Chassis:  system  Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 78. 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 Flex System Enterprise Chassis are controlled by the CMM in each Flex System Enterprise Chassis, using the CMM CLI “users command” on page 353 and the “permggroups command” on page 228 or the CMM web interface. If your Flex System configuration includes optional Flex System Manager hardware, users and permission groups for each optional Flex System Manager installation are controlled by the optional Flex System Manager software (see [http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.8731.doc/product\\_page.html](http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.8731.doc/product_page.html) for information).

**Notes:**

- Permission groups are viewed and modified using the “permggroups command” on page 228.
- Users can be backed up as part of the CMM configuration using the “write command” on page 383.
- Users are restored as part of a backed up CMM configuration using the “read command” on page 269.
- 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 27.
- Before you update the firmware for Power Systems compute nodes using the optional Flex System Manager management software, 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 385 for a list of error messages that apply to all commands or “users command errors” on page 452 for a list of error messages that are specific to the users command.

Table 79. users (CMM users) command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display all user profiles</b>	<p>Displays all 84 (maximum) CMM user profiles. Returned user values are:</p> <ul style="list-style-type: none"> <li>• User name</li> <li>• Permission groups</li> <li>• Current number of active sessions</li> <li>• Maximum sessions allowed</li> <li>• State of account (active or inactive)</li> <li>• Password state (expired or not expired)</li> </ul> <p>A list of current user permission groups displays after the list of user profiles.</p>	users	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>
<b>Display active users</b>	<p>Displays all users that are currently logged in to the CMM. Returned values include:</p> <ul style="list-style-type: none"> <li>• User name</li> <li>• Session ID</li> <li>• Inactive time for each connection</li> <li>• User IP address</li> <li>• Connection type</li> </ul>	users -curr	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>



Table 79. users (CMM users) command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Terminate user session</b>	Terminates the specified user login session. <b>Note:</b> The session ID is found by running the users -curr command.	users -ts <i>sessionID</i> where <i>sessionID</i> is a number that corresponds to the user session ID.  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Display single user profile</b>	Displays the specified CMM user profile. Returned values are: <ul style="list-style-type: none"> <li>• Permission groups</li> <li>• Current number of active sessions</li> <li>• Maximum sessions allowed</li> <li>• State of account (active or inactive)</li> <li>• Password state (expired or not expired)</li> </ul> <b>Note:</b> User names are not case sensitive.	users -n <i>user_name</i> where <i>user_name</i> is a user name assigned in the "Display all user profiles" list.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Disable user profile</b>	Disables the specified CMM user profile. <b>Note:</b> User names are not case sensitive.	users -disable -n <i>user_name</i> where <i>user_name</i> is a user name assigned in the "Display all user profiles" list.  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 79. users (CMM users) command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Enable user profile</b>	Enables a specified CMM user profile that is disabled. <b>Note:</b> User names are not case sensitive.	users -enable -n <i>user_name</i> where <i>user_name</i> is a user name assigned in the "Display all user profiles" list.  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Unlock user profile</b>	Unlocks a specified CMM user profile that is locked. <b>Note:</b> User names are not case sensitive.	users -unlock -n <i>user_name</i> where <i>user_name</i> is a user name assigned in the "Display all user profiles" list.  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Delete user profile</b>	Delete the specified CMM user profile. <b>Note:</b> User names are not case sensitive.	users -clear -n <i>user_name</i> where <i>user_name</i> is a user name assigned in the "Display all user profiles" list.  This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> </ul> See "Commands and user authority" on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 79. users (CMM users) command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<p><b>Add user</b></p>	<p>Create the specified CMM user. The following user-profile fields are required:</p> <ul style="list-style-type: none"> <li>• -n <i>user_name</i></li> <li>• -p <i>user_password</i></li> <li>• -g <i>permission_group</i></li> <li>• -ms <i>max_sessions</i></li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• User names and group names are not case sensitive.</li> <li>• Passwords are case sensitive.</li> </ul>	<pre>users -add -n <i>user_name</i> -p <i>user_password</i> -g <i>permission_group</i> -ms <i>max_sessions</i></pre> <p>where:</p> <ul style="list-style-type: none"> <li>• <i>user_name</i> 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.</li> <li>• <i>user_password</i> 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.</li> <li>• <i>permission_group</i> 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.</li> <li>• <i>max-session</i> 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.</li> </ul> <p>(continued on next page)</p>	<p>Primary CMM:</p> <pre>mm[p] mm[P] mm[x]</pre> <p>where x is the primary CMM bay number.</p>

Table 79. users (CMM users) command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Add user</b> (continued)		This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> </ul> See "Commands and user authority" on page 10 for additional information.	
<b>Change user password (own password)</b>	Allows a user to change the user password in their own CMM user profile. <b>Notes:</b> <ul style="list-style-type: none"> <li>• 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.</li> <li>• User names are not case sensitive.</li> <li>• Passwords are case sensitive.</li> </ul>	users -n <i>user_name</i> -op <i>old_password</i> -p <i>new_password</i> where: <ul style="list-style-type: none"> <li>• <i>user_name</i> is your own user name assigned in the "Display all user profiles" list.</li> <li>• <i>old_password</i> is your current user password. Passwords are case sensitive.</li> <li>• <i>new_password</i> 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.</li> </ul> Users who do not have authority to manage accounts can change their own password using the -op option.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 79. users (CMM users) command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<p><b>Change user password (other user)</b></p>	<p>Forces a password change in the specified CMM user profile.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• User names are not case sensitive.</li> <li>• Passwords are case sensitive.</li> <li>• Users can change their own password, even if they do not have authority to manage accounts, by specifying the <code>-op</code> option (see the <code>users -op</code> command description for information).</li> </ul>	<p><code>users -n user_name -p new_password</code>            where:</p> <ul style="list-style-type: none"> <li>• <code>user_name</code> is a user name assigned in the "Display all user profiles" list.</li> <li>• <code>new_password</code> 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.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>
<p><b>Set user permission groups</b></p>	<p>Sets the user permission groups in the specified CMM user profile.</p> <p><b>Note:</b> User names and group names are not case sensitive.</p>	<p><code>users -n user_name -g permission_group</code>            where:</p> <ul style="list-style-type: none"> <li>• <code>user_name</code> is a user name assigned in the "Display all user profiles" list.</li> <li>• <code>permission_group</code> 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.</li> </ul>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>

Table 79. users (CMM users) command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
		<p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	
<p><b>Set maximum number of simultaneous sessions for user</b></p>	<p>Sets the maximum number of simultaneous login sessions for the specified user.</p> <p><b>Note:</b> User names are not case sensitive.</p>	<p><code>users -n <i>user_name</i> -ms <i>max-session</i></code>            where:</p> <ul style="list-style-type: none"> <li>• <i>user_name</i> is a user name assigned in the "Display all user profiles" list.</li> <li>• <i>max-session</i> 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.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where <i>x</i> is the primary CMM bay number.</p>

Table 79. users (CMM users) command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<p><b>Add SSH public key to user</b></p>	<p>Adds an SSH public key to the specified user. The following user-profile fields are required:</p> <ul style="list-style-type: none"> <li>• -n <i>user_name</i></li> <li>• -kf <i>key_format</i></li> <li>• -key <i>key</i></li> </ul>	<p>users -add -n <i>user_name</i> -kf <i>key_format</i> -key "<i>key</i>" where:</p> <ul style="list-style-type: none"> <li>• <i>user_name</i> is a user name assigned in the "Display all user profiles" list.</li> <li>• <i>key_format</i> is openssh</li> <li>• <i>key</i> is an SSH public key, up to 6000 characters in length, enclosed in double-quotes.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>
<p><b>Remove SSH public key from user</b></p>	<p>Removes one or all SSH public keys associated with the specified user.</p>	<p>users -remove -n <i>user_name</i> -ki <i>key_index</i> where:</p> <ul style="list-style-type: none"> <li>• <i>user_name</i> is a user name assigned in the "Display all user profiles" list.</li> <li>• <i>key_index</i> is <ul style="list-style-type: none"> <li>– an integer between 1 and 20 that identifies a key for the specified user.</li> <li>– all to remove all keys associated with the specified user</li> </ul> </li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>

Table 79. users (CMM users) command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<p><b>Import (upload) and add new SSH public key</b></p>	<p>Import (upload) and add a new SSH public key for user. The upload location of the key file, including IP address and filename, an must be set using the -u command option.</p>	<p>users -upld -n <i>user_name</i> -kf <i>key_format</i> -u <i>URL</i>            where:</p> <ul style="list-style-type: none"> <li>• <i>user_name</i> is a user name assigned in the "Display all user profiles" list.</li> <li>• <i>key_format</i> is openssh</li> <li>• <i>URL</i> is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the key file is located.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>
<p><b>Import (upload) and update existing SSH public key</b></p>	<p>Import (upload) and update existing SSH public key for user. The upload location of the key file, including IP address and filename, an must be set using the -u command option.</p>	<p>users -upld -n <i>user_name</i> -ki <i>key_index</i> -kf <i>key_format</i> -u <i>URL</i>            where:</p> <ul style="list-style-type: none"> <li>• <i>user_name</i> is a user name assigned in the "Display all user profiles" list.</li> <li>• <i>key_index</i> is an integer between 1 and 20 that identifies a key for the specified user.</li> <li>• <i>key_format</i> is openssh</li> <li>• <i>URL</i> is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the key file is located.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> </ul>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>



Table 79. users (CMM users) command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
		<ul style="list-style-type: none"> <li>Chassis account management</li> </ul> See "Commands and user authority" on page 10 for additional information.	
<b>Export (download) SSH public key</b>	Export (download) the specified SSH public key. The download location of the key file, including IP address and filename, and must be set using the -u command option.	users -dnld -n <i>user_name</i> -ki <i>key_index</i> -kf <i>key_format</i> -u <i>URL</i> where: <ul style="list-style-type: none"> <li><i>user_name</i> is a user name assigned in the "Display all user profiles" list.</li> <li><i>key_index</i> is an integer between 1 and 20 that identifies a key for the specified user.</li> <li><i>key_format</i> is openssh</li> <li><i>URL</i> is fully qualified uniform resource locator, including file name, of the tftp, ftp, http, https, or sftp server where the key file is located.</li> </ul>	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Display SSH public key information (summary)</b>	Displays SSH public key information summary for the specified user.	users -u <i>user_name</i> -ki <i>key_index</i> where: <ul style="list-style-type: none"> <li><i>user_name</i> is a user name assigned in the "Display all user profiles" list.</li> <li><i>key_index</i> is               <ul style="list-style-type: none"> <li>an integer between 1 and 20 that identifies a key for the specified user.</li> <li>all to display all keys associated with the specified user</li> </ul> </li> </ul>	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Display complete SSH public key information</b>	Displays complete SSH public key information for the specified user. <b>Note:</b> When displaying complete key information, you can only specify one key index each time you run the command.	users -u <i>user_name</i> -ki <i>key_index</i> -kf <i>key_format</i> -e where: <ul style="list-style-type: none"> <li><i>user_name</i> is a user name assigned in the "Display all user profiles" list.</li> <li><i>key_index</i> is               <ul style="list-style-type: none"> <li>an integer between 1 and 20 that identifies a key for the specified user.</li> </ul> </li> <li><i>key_format</i> is openssh</li> </ul>	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 79. users (CMM users) command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<p><b>Update SSH public key</b></p>	<p>Updates the information for the specified SSH public key for the specified user. Information that can be updated includes:</p> <ul style="list-style-type: none"> <li>• The list of hosts from which the specified user will accept connections.</li> <li>• Comments.</li> </ul>	<p>users -n <i>user_name</i> -ki <i>key_index</i> -kf <i>key_format</i> -key "<i>key</i>" -af "<i>host_list</i>" -cm "<i>comment</i>"            where:</p> <ul style="list-style-type: none"> <li>• <i>user_name</i> is a user name assigned in the "Display all user profiles" list.</li> <li>• <i>key_index</i> is an integer between 1 and 20 that identifies a key for the specified user.</li> <li>• <i>key_format</i> is openssh</li> <li>• <i>key</i> is an SSH public key, up to 6000 characters in length, enclosed in double-quotes.</li> <li>• <i>host_list</i> a list of hosts that the specified user will accept connections from, in the format: from="<i>list</i>" where <i>list</i> 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 ( % ).</li> <li>• <i>comment</i> is a string of up to 255 characters in length, enclosed in double-quotes.</li> </ul> <p><i>(continued on next page)</i></p>	<p>Primary CMM:</p> <p>mm[p]            mm[P]            mm[x]            where x is the primary CMM bay number.</p>
<p><b>Update SSH public key</b> <i>(continued)</i></p>		<p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> </ul> <p>See "Commands and user authority" on page 10 for</p>	

Table 79. users (CMM users) command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
		additional information.	
<p><b>Update user SNMPv3 information</b></p>	<p>Updates the SNMPv3 information for the specified user. Information that can be updated includes:</p> <ul style="list-style-type: none"> <li>• Context name</li> <li>• Authentication protocol</li> <li>• Privacy protocol</li> <li>• Privacy password</li> <li>• Access type</li> <li>• IP address of the SNMPv3 server</li> </ul> <p><b>Note:</b> SNMPv3 related command options can also be modified singly for each specified user.</p>	<p>users -n <i>user_name</i> -cn "<i>context_name</i>" -ap <i>authentication_protocol</i> -pp <i>privacy_proto</i> -ppw <i>privacy_pwd</i> -at <i>access_type</i> -i <i>hostname/ip_address</i></p> <p>where:</p> <ul style="list-style-type: none"> <li>• <i>user_name</i> is a user name assigned in the "Display all user profiles" list.</li> <li>• <i>context_name</i> is a unique string up to 32 characters in length, enclosed in double-quotes.</li> <li>• <i>authentication_protocol</i> is md5 or sha .</li> <li>• <i>privacy_proto</i> is des , aes , or none .</li> <li>• <i>privacy_pwd</i> 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 <i>privacy_pwd</i> can be cleared by setting its value to null.</li> <li>• <i>access_type</i> is get , set , or trap .</li> <li>• <i>hostname/ip_address</i> is the host name or IP address of the SNMPv3 server. The <i>hostname/ip_address</i> can be cleared by setting its value to null.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis account management</li> </ul> <p>See "Commands and user authority" on page 10 for</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>

Table 79. users (CMM users) command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
		additional information.	
<p><b>Enable compute node account management by CMM</b></p>	<p>Enables management of compute node IPMI and SNMPv3 user accounts by the CMM. This command option allows the CMM user accounts to be used for managing most compute nodes in the chassis instead of having the Flex System Manager user accounts used to manage the compute nodes.</p> <p><b>Important:</b> Management of compute node IPMI and SNMPv3 user accounts is not supported by POWER-based compute nodes.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>Enabling CMM management of IPMI/SNMPv3 user accounts 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.</li> <li>Once enabled, the only way to disable the users -am enabled command option is to reset the CMM to manufacturing defaults using the "clear command" on page 91 or using the fsmcm -off command (see "fsmcm command" on page 137).</li> </ul>	<p>users -am enabled</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis account management</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where x is the primary CMM bay number.</p>

Table 79. users (CMM users) command (continued)

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Enable / disable IPMI and SNMPv3 centralized management</b>	<p>Enables or disables centralized management of IPMI and SNMPv3 user accounts, including user provisioning.</p> <p>This command enables you to control whether or not specific CMM user accounts can be used to manage chassis components (including provisioning). Remember that enabling a user account will not actually allow local management of chassis components unless you have enabled compute node management by the CMM using the <code>users -am enabled</code> command option.</p> <p><b>Note:</b> 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.</p>	<p><code>users -ipmisnmpv3 state -n user_name</code>                      where:</p> <ul style="list-style-type: none"> <li><code>state</code> is enabled or disabled .</li> <li><code>user_name</code> is a user name assigned in the "Display all user profiles" list.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis account management</li> </ul> <p>See "Commands and user authority" on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p]                      mm[P]                      mm[x]                      where x is the primary CMM bay number.</p>

**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 Flex System components, as defined by the "permggroups command" on page 228), 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 AAAAB3NzaC1yc2EAAAABIwAAAQEA... 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 AAAAB3NzaC1yc2EAAAABIwAAAQEA..."
```

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 passwd -g super -ms 10
```

```
OK
```

```
system:mm[2]> users
```

```
-am enabled
```

```
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 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 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 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
-ipmismnmpv3 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 AAAAB3NzaC1yc2EAAAAB
BIwAAAEAvfnTUzRF7pdBuaBy4d0/aIFasa/Gtc+o/wLZnuC4aDHMA1UmnMyL0CiIaN0y400ICEKcQ
jKEhrYymtAoVtfkApvY39GpnSGRC/qcLGWLM4cmirKL5kxHNOqIcwbT1NPceoKHj46X7E+mqlfWnAh
hjDpcVFjagM3Ek2y7w/tBGrwGgN7DPHJU1tzCjy68mEAnIrzjUoR98Q3/B9cJD77ydGKe8rPdI2hIE
pXR5dNUiupA1Yd8PSSMgdukASKEd3eRRZTBl3SAAtMucUsTkYjLXcqex10Qz4+N50R6MbNcwlSx+mTE
AvvcPJhuga70UNPGhLJML6k7jeJiQ8Xd2pXb0ZQ=="
OK
```

```
system:mm[2]> users -n test
-g opmin
-ms 5
-cn admin
-ap sha
-pp des
-at set
-i 0.0.0.0
-ipmismnpv3 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 AAAAB3NzaC1yc2EAAAABIwAAAQEAfnTUzRF7pdBuaBy4d0/aIFasa/Gtc+o/wlZnuC4aD
HMA1UmnMyLOCiIaNOy400ICEKcjqKEhrYymtAoVtfKApvY39GpnSGRC/qcLGWLM4cmirKL5kxHNOqI
cwbT1NPceoKHj46X7E+mqlfWnAhhjDpcVFjagM3Ek2y7w/tBGrwGgN7DPHJU1tzcJy68mEAnIrzjUo
R98Q3/B9cJD77ydGKe8rPdI2hIEpXR5dNUiupA1Yd8PSSMgdukASKEd3eRRZTBL3SAtMucUsTkYjLX
cqex10Qz4+N50R6MbNcwlxsx+mTEAvvcPJhuga70UNPGhLJML6k7jeJiQ8Xd2pXbOZQ==
```

```
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 385 for a list of error messages that apply to all commands or “vlan command errors” on page 456 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 80. vlan command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display all VLAN settings</b>	Displays all VLAN settings for specified command target. <b>Note:</b> 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:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Display VLAN settings for specific VLAN ID</b>	Displays VLAN settings for the specified VLAN ID of the command target.	vlan -vi <i>index</i> where <i>index</i> is the VLAN entry index number.	Flex System Enterprise Chassis:  system  Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Apply CMM VLAN settings</b>	Applies changes made to the CMM VLAN configuration. <b>Note:</b> You must commit CMM VLAN configuration changes before the commit timeout expires or the previous configuration is restored.	vlan -commit This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 80. *vlan* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>CMM commit timeout</b>	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.	<p><i>vlan -cto timeout</i> where <i>timeout</i> is from 1 to 255 minutes, inclusive.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where <i>x</i> is the primary CMM bay number.</p>
<b>Set global VLAN state</b>	<p>Enables or disables the global VLAN state.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• The value of the global VLAN state does not change individual VLAN settings.</li> <li>• All changes to the CMM configuration must be applied using the <i>vlan -commit</i> command option, before the commit timeout expires.</li> </ul>	<p><i>vlan -state state</i> where <i>state</i> is</p> <ul style="list-style-type: none"> <li>• enabled</li> <li>• disabled</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where <i>x</i> is the primary CMM bay number.</p>

Table 80. *vlan* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Set VLAN state for non-fixed entry</b></p>	<p>Sets the VLAN state of the specified non-fixed entry.</p> <p><b>Note:</b> All changes to the CMM configuration must be applied using the <code>vlan -commit</code> command option, before the commit timeout expires.</p>	<p><code>vlan -vi <i>index</i> -state <i>state</i></code>            where</p> <ul style="list-style-type: none"> <li>• <i>index</i> is the VLAN entry index number.</li> <li>• <i>state</i> is               <ul style="list-style-type: none"> <li>– enabled</li> <li>– disabled</li> <li>– restart</li> </ul> </li> </ul> <p>This command can only be run by users who have one or more of the following command authorities.</p> <ul style="list-style-type: none"> <li>• For the Flex System Enterprise Chassis target:               <ul style="list-style-type: none"> <li>– Supervisor</li> <li>– Blade configuration</li> </ul> </li> <li>• For the primary CMM target:               <ul style="list-style-type: none"> <li>– Supervisor</li> <li>– Chassis configuration</li> </ul> </li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Flex System Enterprise Chassis:                system</p> <p>Primary CMM:                mm[p]                mm[P]                mm[x]                where x is the primary CMM bay number.</p>
<p><b>Delete all non-fixed VLAN entries</b></p>	<p>Deletes all non-fixed VLAN entries.</p> <p><b>Note:</b> All changes to the CMM configuration must be applied using the <code>vlan -commit</code> command option, before the commit timeout expires.</p>	<p><code>vlan -delete</code>            This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:                mm[p]                mm[P]                mm[x]                where x is the primary CMM bay number.</p>

Table 80. *vlan* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Delete specific VLAN entry</b>	<p>Deletes the specified VLAN entry.</p> <p><b>Note:</b> All changes to the CMM configuration must be applied using the <code>vlan -commit</code> command option, before the commit timeout expires.</p>	<p><code>vlan -vi <i>index</i> -delete</code> where <i>index</i> is the VLAN entry index number.</p> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where <i>x</i> is the primary CMM bay number.</p>
<b>Create VLAN entry</b>	<p>Creates the specified VLAN entry.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• <code>-vi</code> and <code>-vid</code> must both be set to create an entry.</li> <li>• The <code>-state</code> and <code>-n</code> (name) are set as optional parameters.</li> <li>• A default entry name is used if <code>-n</code> is not specified.</li> <li>• All changes to the CMM configuration must be applied using the <code>vlan -commit</code> command option, before the commit timeout expires.</li> </ul>	<p><code>vlan -vi <i>index</i> -vid <i>vlan_id</i></code> where</p> <ul style="list-style-type: none"> <li>• <i>index</i> is an unused VLAN entry index number.</li> <li>• <i>vlan_id</i> is the number from 1 to 4,094, inclusive.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities.</p> <ul style="list-style-type: none"> <li>• For the Flex System Enterprise Chassis target:               <ul style="list-style-type: none"> <li>– Supervisor</li> <li>– Blade configuration</li> </ul> </li> <li>• For the primary CMM target:               <ul style="list-style-type: none"> <li>– Supervisor</li> <li>– Chassis configuration</li> </ul> </li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Flex System Enterprise Chassis:</p> <p><code>system</code></p> <p>Primary CMM:</p> <p><code>mm[p]</code>  <code>mm[P]</code>  <code>mm[x]</code>            where <i>x</i> is the primary CMM bay number.</p>

Table 80. *vlan* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Set VLAN ID</b></p>	<p>Sets a new ID for the specified VLAN entry.</p> <p><b>Note:</b> All changes to the CMM configuration must be applied using the <code>vlan -commit</code> command option, before the commit timeout expires.</p>	<p><code>vlan -vi <i>index</i>-vid <i>id</i></code> where</p> <ul style="list-style-type: none"> <li><i>index</i> is the VLAN entry index number.</li> <li><i>id</i> is the number from 1 to 4,094, inclusive.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities.</p> <ul style="list-style-type: none"> <li>For the Flex System Enterprise Chassis target: <ul style="list-style-type: none"> <li>Supervisor</li> <li>Blade configuration</li> </ul> </li> <li>For the primary CMM target: <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> </li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Flex System Enterprise Chassis:</p> <p>system</p> <p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where <i>x</i> is the primary CMM bay number.</p>
<p><b>Set SOL access state</b></p>	<p>Enables or disables SOL access for the specified VLAN entry.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>Before enabling SOL access, you must first to disable it on the VLAN where it is enabled.</li> <li>If only one VLAN is in use, you cannot disable SOL access.</li> <li>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.</li> <li>All changes to the CMM configuration must be applied using the <code>vlan -commit</code> command option, before the commit timeout expires.</li> </ul>	<p><code>vlan -vi <i>index</i>-sol <i>state</i></code> where</p> <ul style="list-style-type: none"> <li><i>index</i> is the VLAN entry index number.</li> <li><i>state</i> is enabled or disabled.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where <i>x</i> is the primary CMM bay number.</p>

Table 80. *vlan* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Set VLAN tagging state (fixed entry)</b>	Enables or disabled VLAN tagging for the default (fixed) entry. <b>Note:</b> All changes to the CMM configuration must be applied using the <code>vlan -commit</code> command option, before the commit timeout expires.	<code>vlan -vi index-tag state</code> where <ul style="list-style-type: none"> <li><code>index</code> is 1 (the fixed VLAN entry index number).</li> <li><code>state</code> is enabled or disabled.</li> </ul> This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  <code>mm[p]</code> <code>mm[P]</code> <code>mm[x]</code> where <code>x</code> is the primary CMM bay number.
<b>Set VLAN entry name</b>	Sets a name for the specified VLAN entry. <b>Note:</b> All changes to the CMM configuration must be applied using the <code>vlan -commit</code> command option, before the commit timeout expires.	<code>vlan -vi index-n name</code> where <ul style="list-style-type: none"> <li><code>index</code> is the VLAN entry index number.</li> <li><code>name</code> is the quote-delimited VLAN entry name, of 1 to 31 characters in length.</li> <li>For the Flex System Enterprise Chassis target:                             <ul style="list-style-type: none"> <li>Supervisor</li> <li>Blade configuration</li> </ul> </li> <li>For the primary CMM target:                             <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> </li> </ul>	Flex System Enterprise Chassis:  <code>system</code>  Primary CMM:  <code>mm[p]</code> <code>mm[P]</code> <code>mm[x]</code> where <code>x</code> is the primary CMM bay number.
<b>Set VLAN IPv4 configuration method to static</b>	Sets the IPv4 configuration method for the specified VLAN non-fixed entry to static. <b>Note:</b> All changes to the CMM configuration must be applied using the <code>vlan -commit</code> command option, before the commit timeout expires.	<code>vlan -vi index-c method</code> where <ul style="list-style-type: none"> <li><code>index</code> is the VLAN entry index number.</li> <li><code>method</code> is static.</li> </ul> This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  <code>mm[p]</code> <code>mm[P]</code> <code>mm[x]</code> where <code>x</code> is the primary CMM bay number.

Table 80. *vlan* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Set VLAN IP address (IPv4)</b>	Sets the IPv4 address for the specified VLAN non-fixed entry. <b>Note:</b> All changes to the CMM configuration must be applied using the <code>vlan -commit</code> command option, before the commit timeout expires.	<code>vlan -vi index-i ip_address</code> where <ul style="list-style-type: none"> <li>• <i>index</i> is the VLAN entry index number.</li> <li>• <i>ip_address</i> is a valid IPv4 IP address.</li> </ul> This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  <code>mm[p]</code> <code>mm[P]</code> <code>mm[x]</code> where <i>x</i> is the primary CMM bay number.
<b>Set VLAN subnet (IPv4)</b>	Sets the IPv4 subnet for the specified VLAN non-fixed entry. <b>Note:</b> All changes to the CMM configuration must be applied using the <code>vlan -commit</code> command option, before the commit timeout expires.	<code>vlan -vi index-s subnet</code> where <ul style="list-style-type: none"> <li>• <i>index</i> is the VLAN entry index number.</li> <li>• <i>subnet</i> is the IPv4 subnet.</li> </ul> This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  <code>mm[p]</code> <code>mm[P]</code> <code>mm[x]</code> where <i>x</i> is the primary CMM bay number.
<b>Set VLAN gateway (IPv4)</b>	Sets the IPv4 gateway for the specified VLAN non-fixed entry. <b>Note:</b> All changes to the CMM configuration must be applied using the <code>vlan -commit</code> command option, before the commit timeout expires.	<code>vlan -vi index-g gateway</code> where <ul style="list-style-type: none"> <li>• <i>index</i> is the VLAN entry index number.</li> <li>• <i>gateway</i> is the IPv4 gateway.</li> </ul> This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  <code>mm[p]</code> <code>mm[P]</code> <code>mm[x]</code> where <i>x</i> is the primary CMM bay number.

Table 80. *vlan* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<p><b>Set VLAN IPv4 subnet route</b></p>	<p>Sets a custom value for the specified IPv4 subnet route of the specified VLAN non-fixed entry.</p> <p><b>Note:</b> All changes to the CMM configuration must be applied using the <code>vlan -commit</code> command option, before the commit timeout expires.</p>	<p><code>vlan -vi index-sr xsubnet_route</code> where</p> <ul style="list-style-type: none"> <li><code>index</code> is the VLAN entry index number.</li> <li><code>x</code> is the subnet route number 1, 2, or 3.</li> <li><code>subnet_route</code> is the IPv4 subnet route.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where <i>x</i> is the primary CMM bay number.</p>
<p><b>Set VLAN IPv4 subnet mask</b></p>	<p>Sets a custom value for the specified IPv4 subnet mask for the specified VLAN non-fixed entry.</p> <p><b>Note:</b> All changes to the CMM configuration must be applied using the <code>vlan -commit</code> command option, before the commit timeout expires.</p>	<p><code>vlan -vi index-sm xsubnet_mask</code> where</p> <ul style="list-style-type: none"> <li><code>index</code> is the VLAN entry index number.</li> <li><code>x</code> is the subnet route number 1, 2, or 3.</li> <li><code>subnet_mask</code> is the IPv4 subnet mask.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	<p>Primary CMM:</p> <p>mm[p] mm[P] mm[x] where <i>x</i> is the primary CMM bay number.</p>



Table 80. *vlan* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Set VLAN IPv6 configuration method to static</b>	Sets the IPv6 configuration method for the specified VLAN non-fixed entry to static.	<p><code>vlan -vi <i>index</i> -c6 <i>method</i></code> where</p> <ul style="list-style-type: none"> <li><i>index</i> is the VLAN entry index number.</li> <li><i>method</i> is static.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	Primary CMM:  <code>mm[p]</code> <code>mm[P]</code> <code>mm[x]</code> where <i>x</i> is the primary CMM bay number.
<b>Set VLAN IP address (IPv6)</b>	Sets the IPv6 address for the specified VLAN non-fixed entry. <b>Note:</b> All changes to the CMM configuration must be applied using the <code>vlan -commit</code> command option, before the commit timeout expires.	<p><code>vlan -vi <i>index</i> -i6 <i>ip_address</i></code> where</p> <ul style="list-style-type: none"> <li><i>index</i> is the VLAN entry index number.</li> <li><i>ip_address</i> is a valid IPv6 IP address.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	Primary CMM:  <code>mm[p]</code> <code>mm[P]</code> <code>mm[x]</code> where <i>x</i> is the primary CMM bay number.
<b>Set VLAN IPv6 prefix length</b>	Sets the IPv6 prefix length for the specified VLAN non-fixed entry. <b>Note:</b> All changes to the CMM configuration must be applied using the <code>vlan -commit</code> command option, before the commit timeout expires.	<p><code>vlan -vi <i>index</i> -p6 <i>prefix_length</i></code> where</p> <ul style="list-style-type: none"> <li><i>index</i> is the VLAN entry index number.</li> <li><i>prefix_length</i> is the IPv6 prefix length.</li> </ul> <p>This command can only be run by users who have one or more of the following command authorities:</p> <ul style="list-style-type: none"> <li>Supervisor</li> <li>Chassis configuration</li> </ul> <p>See “Commands and user authority” on page 10 for additional information.</p>	Primary CMM:  <code>mm[p]</code> <code>mm[P]</code> <code>mm[x]</code> where <i>x</i> is the primary CMM bay number.

Table 80. *vlan* command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Set VLAN gateway (IPv6)</b>	Sets the IPv6 gateway for the specified VLAN non-fixed entry. <b>Note:</b> All changes to the CMM configuration must be applied using the <code>vlan -commit</code> command option, before the commit timeout expires.	<code>vlan -vi index-g6 gateway</code> where <ul style="list-style-type: none"> <li>• <i>index</i> is the VLAN entry index number.</li> <li>• <i>gateway</i> is the IPv6 gateway.</li> </ul> This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Set VLAN IPv6 subnet route</b>	Sets a custom value for the specified IPv6 subnet route of the specified VLAN non-fixed entry. <b>Note:</b> All changes to the CMM configuration must be applied using the <code>vlan -commit</code> command option, before the commit timeout expires.	<code>vlan -vi index-sr6 xsubnet_route</code> where <ul style="list-style-type: none"> <li>• <i>index</i> is the VLAN entry index number.</li> <li>• <i>x</i> is the subnet route number 1, 2, or 3.</li> <li>• <i>subnet_route</i> is the IPv6 subnet route.</li> </ul> This command can only be run by users who have one or more of the following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.
<b>Set VLAN IPv6 subnet prefix length</b>	Sets a custom value for the specified IPv6 subnet prefix length for the specified VLAN non-fixed entry. <b>Note:</b> All changes to the CMM configuration must be applied using the <code>vlan -commit</code> command option, before the commit timeout expires.	<code>vlan -vi index-sp6 xprefix_length</code> where <ul style="list-style-type: none"> <li>• <i>index</i> is the VLAN entry index number.</li> <li>• <i>x</i> is the subnet route number 1, 2, or 3.</li> <li>• <i>prefix_length</i> is the IPv6 subnet prefix length.</li> </ul> This command can only be run by users who have one or more of the	Primary CMM:  mm[p] mm[P] mm[x] where x is the primary CMM bay number.

Table 80. vlan command (continued)

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
		following command authorities: <ul style="list-style-type: none"> <li>• Supervisor</li> <li>• Chassis configuration</li> </ul> See “Commands and user authority” on page 10 for additional information.	

**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 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 385 for a list of error messages that apply to all commands or “volts command errors” on page 459 for a list of error messages that are specific to the volts command.

Table 81. volts command

Function	What it does	Command	Target (see paths in “Command targets” on page 6)
<b>Display voltage values</b>	Displays the current voltage and voltage threshold settings for the specified compute node. <b>Note:</b> The voltage values that display will vary based on chassis and compute node type.	volts	Compute node:  blade[x] 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 Flex System Enterprise 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 269.

### 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 27.

If command syntax is not correctly entered, or if a command fails to run, an error message is returned. See “Common errors” on page 385 for a list of error messages that apply to all commands or “write command errors” on page 459 for a list of error messages that are specific to the write command.

Table 82. write command

Function	What it does	Command	Target (see paths in "Command targets" on page 6)
<b>Save CMM configuration to file</b>	Saves an image of the CMM configuration to a file. This image includes CMM users and permission groups.	<pre>write -u URL -p passphrase</pre> where: <ul style="list-style-type: none"> <li>• <i>URL</i> 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.</li> <li>• "<i>passphrase</i>" 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.</li> </ul>	Primary CMM:  mm[p] mm[P] mm[x] 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 Flex System Enterprise 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]
```

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 and a passphrase of Passphaase, while the Flex System Enterprise 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 these commands:

```
system> write -u tftp://9.37.177.215/temp/cmm1.cfg -p "backuplock" -T mm[p]
OK
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 Flex SystemChassis Management Module 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 83. Common errors

Error message	Definition
Command cannot be issued to this target. Type <code>env -h</code> 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: <i>option</i> where <i>option</i> 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, <code>dns -i192.168.70.29 -i</code>
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, <code>env -Tsystem : blade[4] -Tsystem : blade[5]</code> .
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 - <i>option</i> where <i>option</i> 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 <i>option</i> where <i>option</i> 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 <i>option</i> for the target. where <i>option</i> identifies the option that is invalid.	A user tries to issue a command with an invalid option for the target.
Illegal option: <i>option</i> where <i>option</i> identifies the illegal short command option that was entered.	A user tries to enter an illegal short command option.

Table 83. Common errors (continued)

Error message	Definition
Integer argument out of range ( <i>range - range</i> ) for <i>-option: argument</i> where: <ul style="list-style-type: none"> <li>• <i>range</i> identifies the range limits</li> <li>• <i>option</i> identifies the command option</li> <li>• <i>argument</i> identifies the integer that is out of range</li> </ul>	A user tries to enter an integer argument that is out of range.
Internal error.	An internal error occurs.
Invalid integer argument for <i>-option: argument</i> where: <ul style="list-style-type: none"> <li>• <i>option</i> identifies the command option</li> <li>• <i>argument</i> identifies the invalid argument</li> </ul>	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 <i>option: argument</i> where: <ul style="list-style-type: none"> <li>• <i>option</i> identifies the command option</li> <li>• <i>argument</i> identifies the invalid argument</li> </ul>	A user tries to enter an invalid argument for the specified command option.
Invalid option argument for <i>option: arguments</i> containing spaces must be enclosed in quotation marks. where <i>option</i> 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: <i>option</i> where <i>option</i> 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 <i>command - h</i> for help. where <i>command</i> 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 <i>option</i> requires an argument where <i>option</i> 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 <i>option</i> exceeds max length ( <i>max</i> characters): <i>argument</i> where: <ul style="list-style-type: none"> <li>• <i>option</i> identifies the option that has an argument of excessive length.</li> <li>• <i>max</i> is the maximum allowed argument length.</li> <li>• <i>argument</i> is the argument that was entered.</li> </ul>	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 <i>option</i> requires an argument where <i>option</i> identifies the short command option that is missing an argument.	A short command option is entered without a required argument.
Syntax error. Type <i>command -h</i> for help. where <i>command</i> identifies the command that is returning an error.	A user tries to enter a command improperly.



Table 83. Common errors (continued)

Error message	Definition
The argument for option <i>option</i> is outside the valid range. where <i>option</i> 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 <i>option</i> is outside the valid range of <i>minimum - maximum</i> where: <ul style="list-style-type: none"> <li><i>option</i> identifies the command option that has an out of range argument.</li> <li><i>minimum</i> is the smallest allowed value</li> <li><i>maximum</i> is the largest allowed value</li> </ul>	A user tries to enter an argument that is outside of the valid range for the option.
The argument for option <i>option</i> must be numeric. where <i>option</i> 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 <code>env - Tsystem : blade[15]</code> command is out of range because the Flex System Enterprise 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: <i>option</i> where <i>option</i> identifies the command option that is unknown.	A user tries to enter a long option that is not valid for the command.
Unknown option: <i>option</i> where <i>option</i> identifies the command option that is unknown.	A user tries to enter an unknown command option.
Unrecognized long option: <i>option</i> where <i>option</i> 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.

## accsecfg command errors

This topic lists error messages for the accsecfg command.

See “Common errors” on page 385 for a list of error messages that apply to all commands. See “accseccfg command” on page 35 for information about command syntax and examples of command use.

Table 84. accsecfg 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 84. *accsecfcfg* command errors (continued)

Error message	Definition
The minimum password change interval must be less than the password expiration period ( <i>number</i> days or <i>number</i> hours), where <i>number</i> 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 ( <i>number</i> days or <i>number</i> hours) must be greater than the minimum password change interval, where <i>number</i> 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 385 for a list of error messages that apply to all commands. See “advfailover command” on page 45 for information about command syntax and examples of command use.

Table 85. *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 Flex System Enterprise Chassis.

## airfilter command errors

This topic lists errors for the airfilter command.

See “Common errors” on page 385 for a list of error messages that apply to all commands. See “airfilter command” on page 47 for information about command syntax and examples of command use.

Table 86. *airfilter* command errors

Error message	Definition
Error reading air filter settings	An error occurs while the CMM is reading the air filter settings.

## 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 385 for a list of error messages that apply to all commands. See “alertcfg command” on page 48 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 385 for a list of error messages that apply to all commands. See “alertentries command” on page 50 for information about command syntax and examples of command use.

Table 87. 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.
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 385 for a list of error messages that apply to all commands. See “autoftp command” on page 57 for information about command syntax and examples of command use.

Table 88. 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.

Table 88. *autoftp* command errors (continued)

Error message	Definition
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 385 for a list of error messages that apply to all commands. See “baydata command” on page 59 for information about command syntax and examples of command use.

Table 89. *baydata* command errors

Error message	Definition
Error writing bay data to blade bay <i>bay</i> where <i>bay</i> is the node bay number.	An error occurs while writing to the identified compute node.
Error writing bay data to blade bay <i>bay:slot</i> where <i>bay</i> is the node bay number and <i>slot</i> 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 <i>number</i> where <i>number</i> is the node bay number.	A user attempts to direct a command to a bay that does not contain a compute node.

Table 89. baydata command errors (continued)

Error message	Definition
No blade is present in bay <i>bay:slot</i> where <i>bay</i> is the node bay number and <i>slot</i> 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 <i>bay</i> where <i>bay</i> 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 385 for a list of error messages that apply to all commands. See “bootmode command” on page 64 for information about command syntax and examples of command use.

Table 90. bootmode command errors

Error message	Definition
Boot mode not supported on blade[ <i>x</i> ] where <i>x</i> 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.
Set the blade <i>bay</i> boot mode to permanent failed where <i>bay</i> 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 <i>bay</i> boot mode to temporary failed where <i>bay</i> 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 385 for a list of error messages that apply to all commands. See “bootseq command” on page 66 for information about command syntax and examples of command use.

Table 91. 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[ <i>x</i> ] where <i>x</i> identifies the compute node.	The user tries to enter a boot sequence that is not valid for the compute node target.

Table 91. *bootseq* command errors (continued)

Error message	Definition
Boot sequences exceeds max of <i>max_boot_seqs</i> where <i>max_boot_seqs</i> 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 where <i>x</i> identifies the compute node.	An error occurs while the CMM is processing the command.
Device not found for <i>id</i> where <i>id</i> 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 where <i>x</i> identifies the compute node.	An error occurs while the CMM is processing the command.
Getting boot sequence of blade[x] failed where <i>x</i> 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 where <i>x</i> 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 385 for a list of error messages that apply to all commands. See “*chconfig* command” on page 69 for information about command syntax and examples of command use.

Table 92. *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.

Table 92. *chconfig* command errors (continued)

Error message	Definition
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.
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.



Table 92. *chconfig* command errors (continued)

Error message	Definition
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 385 for a list of error messages that apply to all commands. See “*chlog* command ” on page 76 for information about command syntax and examples of command use.

Table 93. *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 <i>number</i> was not found. where <i>number</i> 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.

Table 93. *chlog* command errors (continued)

Error message	Definition
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 385 for a list of error messages that apply to all commands. See “*chmanual* command” on page 79 for information about command syntax and examples of command use.

Table 94. *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.
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 385 for a list of error messages that apply to all commands. See “*cimsub* command” on page 81 for information about command syntax and examples of command use.

Table 95. *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 385 for a list of error messages that apply to all commands. See “cin command ” on page 84 for information about command syntax and examples of command use.

Table 96. 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.
CIN command failed.	An error occurs while the CMM is executing a CIN command.
cin <i>-index -en state</i> cannot be used with other options. where <ul style="list-style-type: none"> <li>• <i>index</i> identifies the cin index entry</li> <li>• <i>state</i> is on or off</li> </ul>	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.

Table 96. *cin* command errors (continued)

Error message	Definition
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 385 for a list of error messages that apply to all commands. See “*cinstatus* command” on page 90 for information about command syntax and examples of command use.

Table 97. *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 385 for a list of error messages that apply to all commands. See “*clear* command” on page 91 for information about command syntax and examples of command use.

Table 98. *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.

Table 98. *clear* command errors (continued)

Error message	Definition
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 <code>env -h</code> 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 <code>'clear -cnfg -o'</code> 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 <code>clear -cnfg -o</code> 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 <code>'clear -cnfg -o'</code> 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 <code>clear -cnfg -o</code> 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 <code>'clear -cnfg -o'</code> 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 <code>'clear -cnfg -o'</code> 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 <code>clear -cnfg -o</code> override option.

## clearlog command errors

This topic lists error messages for the `clearlog` command.

See “Common errors” on page 385 for a list of error messages that apply to all commands. See “`clearlog` command” on page 93 for information about command syntax and examples of command use.

Table 99. *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 385 for a list of error messages that apply to all commands. See “`config` command” on page 95 for information about command syntax and examples of command use.

Table 100. 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.
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 385 for a list of error messages that apply to all commands. See “console command” on page 100 for information about command syntax and examples of command use.

Table 101. 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[ <i>node_number</i> ] where <i>node_number</i> 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 385 for a list of error messages that apply to all commands. See “coolingzones command” on page 101 for information about command syntax and examples of command use.

Table 102. 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 <i>max</i> where <i>max</i> 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 385 for a list of error messages that apply to all commands. See “crypto command” on page 103 for information about command syntax and examples of command use.

Table 103. *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. 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 tls1.2srv).
-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.
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: <i>node</i> where <i>node</i> 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 <i>number</i> has invalid params where <i>number</i> identifies the slot with invalid parameters.	Other settings prevent the CMM from transitioning to nist800-131a cryptographic mode.



Table 103. *crypto command errors (continued)*

Error message	Definition
FSM User <i>number</i> has non-compliant SNMP properties where <i>number</i> 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 <i>key</i> for user <i>user</i> has invalid length where <i>key</i> identifies the invalid length key and <i>user</i> 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: <i>node</i> where <i>node</i> 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 <i>number</i> has non-compliant SNMP properties where <i>number</i> 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 385 for a list of error messages that apply to all commands. See “date command” on page 106 for information about command syntax and examples of command use.

Table 104. *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.

Table 104. date command errors (continued)

Error message	Definition
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 <i>min</i> and <i>max</i> where <i>min</i> and <i>max</i> define the range of years that is allowed.	A user tries to enter a year that is outside of the allowed range.

## dhcpcinfo command errors

This topic lists errors for the dhcpcinfo command.

See “Common errors” on page 385 for a list of error messages that apply to all commands. See “dhcpcinfo command” on page 108 for information about command syntax and examples of command use.

Table 105. dhcpcinfo 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.
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 dhcpcinfo 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 385 for a list of error messages that apply to all commands. See “displaylog command” on page 112 for information about command syntax and examples of command use.

Table 106. *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: <i>filename</i> where <i>filename</i> 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 <i>URL</i> failed where <i>URL</i> is the location that was entered when the error occurred.	An error occurs when downloading to the specified URL.
Duplicate date filter: <i>filter</i> where <i>filter</i> is the duplicate date filter that was entered.	The user tries to use duplicate date filters.
Duplicate call home filter: <i>filter</i> where <i>filter</i> is N, C, or S.	The user tries to use duplicate call-home filters.
Duplicate severity filter: <i>filter</i> where <i>filter</i> is the duplicate severity filter that was entered.	The user tries to use duplicate severity filters.
Duplicate source filter: <i>filter</i> where <i>filter</i> 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.
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. <i>error_info</i> where <i>error_info</i> 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: <i>filter</i> where <i>filter</i> is the invalid date filter that was entered.	The user tries to use an invalid date filter.
Invalid call home filter: <i>filter</i> where <i>filter</i> is the invalid filter that was entered.	The user tries to use an invalid call-home filter.
Invalid severity filter: <i>filter</i> where <i>filter</i> is the invalid severity filter that was entered.	The user tries to use an invalid severity filter.
Invalid source filter: <i>filter</i> where <i>filter</i> is the invalid source filter that was entered.	The user tries to use an invalid source filter.

Table 106. *displaylog* command errors (continued)

Error message	Definition
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.
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 385 for a list of error messages that apply to all commands. See “`displaysd` command” on page 118 for information about command syntax and examples of command use.

Table 107. *displaysd* command errors

Error message	Definition
-mmstat can not be used with other options	A user tries to use the <code>-mmstat</code> 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.

Table 107. *displaysd* command errors (continued)

<b>Error message</b>	<b>Definition</b>
Downloading to <i>URL</i> failed. where <i>URL</i> 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.
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.

Table 107. *displaysd* 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.

---

## dns command errors

This topic lists error messages for the `dns` command.

See “Common errors” on page 385 for a list of error messages that apply to all commands. See “`dns` command” on page 120 for information about command syntax and examples of command use.

Table 108. *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 385 for a list of error messages that apply to all commands. See “`env` command” on page 124 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 385 for a list of error messages that apply to all commands. See “`ethoverusb` command” on page 129 for information about command syntax and examples of command use.

Table 109. *ethoverusb* command errors

Error message	Definition
Blade SP's command interface on Ethernet-over-USB is not supported on blade <i>node_number</i> where <i>node_number</i> 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 385 for a list of error messages that apply to all commands. See “events command” on page 131 for information about command syntax and examples of command use.

Table 110. *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 <i>max</i> entries. No more events can be added to the list. where <i>max</i> 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 <i>id</i> already exists in Call Home Exclusion List. where <i>id</i> 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 <i>id</i> does not exist in the Call Home Exclusion List. where <i>id</i> 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.
Event <i>id</i> is invalid to be added into Call Home Exclusion List. where <i>id</i> 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 <code>events</code> 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 <code>events</code> 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 385 for a list of error messages that apply to all commands. See “exit command” on page 133 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 385 for a list of error messages that apply to all commands. See “files command” on page 134 for information about command syntax and examples of command use.

Table 111. files command errors

Error message	Definition
Directory does not exist.	The user tries to enter a directory that does not exist.
Error deleting file <i>filename</i> where <i>filename</i> 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 <i>directory</i> . where <i>directory</i> 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.
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 385 for a list of error messages that apply to all commands. See “fod command” on page 135 for information about command syntax and examples of command use.



Table 112. *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 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 385 for a list of error messages that apply to all commands. See “fruactlog command” on page 136 for information about command syntax and examples of command use.

Table 113. *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 385 for a list of error messages that apply to all commands. See “fsmcm command” on page 137 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 385 for a list of error messages that apply to all commands. See “fuelg command” on page 139 for information about command syntax and examples of command use.

Table 114. *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 <i>domain_number</i> can result in an immediate shutdown. where <i>domain_number</i> identifies the power domain.	A power supply fails and the domain in which it is installed loses redundancy. The Flex System Enterprise 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.
Checking if power is preallocated to switch[ <i>number</i> ] failed. where the <i>number</i> 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.

Table 114. *fuelg* command errors (continued)

Error message	Definition
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 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[ <i>node_number</i> ] failed. where <i>node_number</i> 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 [ <i>node_number</i> ] failed. where <i>node_number</i> 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[ <i>number</i> ] failed. where the <i>number</i> identifies the specified power supply.	An error occurs while the CMM is reading data of specified power supply.
Getting name of mm[ <i>number</i> ] failed where the <i>number</i> identifies the specified CMM bay number.	An error occurs while the CMM is reading the CMM name.
Getting power allocation for blade[ <i>node_number</i> ] failed where <i>node_number</i> identifies the compute node.	An error occurs while the CMM is reading the power allocation information of the specified compute node.
Getting power cap level for blade[ <i>node_number</i> ] failed where <i>node_number</i> 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 <i>domain_number</i> failed where <i>domain_number</i> 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[ <i>node_number</i> ] failed. where <i>node_number</i> identifies the compute node.	An error occurs while the CMM is reading the power state of specified compute node.
Getting power values for blower[ <i>number</i> ] failed. where the <i>number</i> 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.

Table 114. *fuelg* command errors (continued)

Error message	Definition
Getting power values for MM[ <i>number</i> ] failed. where the <i>number</i> 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[ <i>number</i> ] failed. where the <i>number</i> 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[ <i>number</i> ] within domain failed. where the <i>number</i> 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 <i>number</i> failed where the <i>number</i> 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 <i>domain_number</i> failed where <i>domain_number</i> identifies the power domain.	An error occurs while the CMM is reading the status of specified domain.
Invalid option for this blade: <i>option</i> where <i>option</i> 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 <i>min</i> and <i>max</i> Watts. where <i>min</i> and <i>max</i> 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 <i>lower_limit</i> and <i>upper_limit</i> where <i>lower_limit</i> and <i>upper_limit</i> 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 <i>lower_limit</i> and <i>upper_limit</i> where <i>lower_limit</i> and <i>upper_limit</i> 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.
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 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.

Table 114. *fuelg* command errors (continued)

Error message	Definition
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 385 for a list of error messages that apply to all commands. See “groups command” on page 150 for information about command syntax and examples of command use.

Table 115. *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 <i>group_name</i> failed where <i>group_name</i> 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 <i>group_name</i> failed where <i>group_name</i> 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.
Group <i>group_name</i> not found where <i>group_name</i> is the group name that was entered.	A user tries to perform an operation on a group name that does not exist.
Group name <i>group_name</i> already existed where <i>group_name</i> is the group name that was entered.	A user tries to enter a group name that already exists.
Groups are full, max of <i>max_num_groups</i> groups reached where <i>max_num_groups</i> 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): <i>number</i> where <i>number</i> 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: <i>number</i> where <i>number</i> 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): <i>device</i> where <i>device</i> is the device that is not valid.	A user tries to specify RBS authority levels without specifying a valid device scope.

Table 115. *groups* command errors (continued)

Error message	Definition
Invalid rbs device: <i>device</i> where <i>device</i> 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: <i>role</i> where <i>role</i> 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 <i>max_length</i> characters. where <i>max_length</i> 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 385 for a list of error messages that apply to all commands. See “health command” on page 156 for information about command syntax and examples of command use.

Table 116. *health* command errors

Error message	Definition
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.
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 385 for a list of error messages that apply to all commands. See “help command” on page 160 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 385 for a list of error messages that apply to all commands. See “history command” on page 163 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 385 for a list of error messages that apply to all commands. See “ifconfig command” on page 164 for information about command syntax and examples of command use.

Table 117. *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] 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] 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.

Table 117. *ifconfig* command errors (continued)

Error message	Definition
-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: <i>error_ID</i> where <i>error_ID</i> 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.
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.



Table 117. *ifconfig* command errors (continued)

Error message	Definition
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 <code>-id</code> only when setting <code>-i6</code> , <code>-p6</code> , or <code>-g6</code>	The user tries to set a value for <code>-id</code> without specifying an additional command option that is needed.
Interface <i>label</i> is not configured correctly where <i>label</i> identifies the interface.	A user tries to enter incorrect configuration information for the identified interface.
Interface <i>option</i> is read-only. where <i>option</i> identifies the command option	The user tries to configure an option parameter that is read-only.
Interface <i>label</i> is read-only. where <i>label</i> identifies the interface.	A user tries to configure an interface that is read only.
Invalid IP arg for <i>option</i> : <i>ip_address</i> . Each byte has to be in the range (0-255) where: <ul style="list-style-type: none"> <li>• <i>option</i> identifies the command option</li> <li>• <i>ip_address</i> identifies the invalid IP address argument</li> </ul>	The user tries to enter an IP address that is out of range. IP addresses must follow the standard format: <i>xxx.xxx.xxx.xxx</i> , where each <i>xxx</i> is a number from 0 to 255.
Invalid IP arg for <i>option</i> : <i>ip_address</i> . Enter 4 bytes separated by 3 dots where: <ul style="list-style-type: none"> <li>• <i>option</i> identifies the command option</li> <li>• <i>ip_address</i> identifies the invalid IP address argument</li> </ul>	The user tries to enter an IP address that is too long. IP addresses must follow the standard format: <i>xxx.xxx.xxx.xxx</i> , where each <i>xxx</i> is a number from 0 to 255.
Invalid IP arg for <i>option</i> : <i>ip_address</i> . Too few bytes where: <ul style="list-style-type: none"> <li>• <i>option</i> identifies the command option</li> <li>• <i>ip_address</i> identifies the invalid IP address argument</li> </ul>	The user tries to enter an IP address with too few bytes. IP addresses must follow the standard format: <i>xxx.xxx.xxx.xxx</i> , where each <i>xxx</i> is a number from 0 to 255.
Invalid IP arg for <i>option</i> : <i>ip_address</i> . Too many bytes where: <ul style="list-style-type: none"> <li>• <i>option</i> identifies the command option</li> <li>• <i>ip_address</i> identifies the invalid IP address argument</li> </ul>	The user tries to enter an IP address with too many bytes. IP addresses must follow the standard format: <i>xxx.xxx.xxx.xxx</i> , where each <i>xxx</i> is a number from 0 to 255.
Invalid IPv6 arg for <i>-option</i> : <i>ip_address</i> where: <ul style="list-style-type: none"> <li>• <i>option</i> identifies the command option</li> <li>• <i>ip_address</i> identifies the invalid IPv6 address argument</li> </ul>	The user tries to enter an IPv6 address with the wrong format.
Invalid MAC arg for <i>option</i> : <i>address</i> . Invalid syntax where: <ul style="list-style-type: none"> <li>• <i>option</i> identifies the command option</li> <li>• <i>address</i> identifies the invalid MAC address argument</li> </ul>	The user tries to enter an invalid MAC address.
Invalid MAC arg for <i>option</i> : <i>address</i> . Multicast addresses not allowed where: <ul style="list-style-type: none"> <li>• <i>option</i> identifies the command option</li> <li>• <i>address</i> identifies the invalid MAC address argument</li> </ul>	The user tries to enter a multicast address.
Invalid MAC arg for <i>option</i> : <i>address</i> . Too few bytes where: <ul style="list-style-type: none"> <li>• <i>option</i> identifies the command option</li> <li>• <i>address</i> identifies the invalid MAC address argument</li> </ul>	The user tries to enter a MAC address with too few bytes.

Table 117. *ifconfig* command errors (continued)

Error message	Definition
Invalid MAC arg for <i>option</i> : <i>address</i> . Too many bytes where: <ul style="list-style-type: none"> <li><i>option</i> identifies the command option</li> <li><i>address</i> identifies the invalid MAC address argument</li> </ul>	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: <i>option</i> where <i>option</i> 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: <i>option</i> where <i>option</i> 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 <i>maximum</i> characters. where <i>maximum</i> 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.
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 <i>option</i> has read-only access for the standby CMM. where <i>option</i> 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. 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: <ul style="list-style-type: none"> <li>enable protected mode for an I/O module when the protected mode status is already active.</li> <li>disable protected mode for an I/O module when the protected mode status is attention or active.</li> </ul>
Re-enabling interface failed.	An error occurs when enabling an interface.

Table 117. *ifconfig* command errors (continued)

Error message	Definition
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.
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 385 for a list of error messages that apply to all commands. See “info command” on page 192 for information about command syntax and examples of command use.

Table 118. *info* command errors

Error message	Definition
-path not supported on switch[bay] 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 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 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 385 for a list of error messages that apply to all commands. See “iocomp command” on page 199 for information about command syntax and examples of command use.

Table 119. iocomp command errors

Error message	Definition
Error reading I/O Compatibility Detail for blade <i>node_number</i> where <i>node_number</i> 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 <i>bay_number</i> where the <i>bay_number</i> identifies the I/O module.	An error occurs while the CMM is reading I/O compatibility for targeted I/O module.
ERROR!!! IOM <i>bay_number</i> reports incorrect width! sw_width = <i>sw_width</i> where <ul style="list-style-type: none"><li>the <i>bay_number</i> identifies the I/O module</li><li><i>sw_width</i> identifies the invalid width</li></ul>	An error occurs while the CMM is reading I/O compatibility for targeted I/O module.
I/O Compatibility Detail of blade <i>node_number</i> : unknown where <i>node_number</i> 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 385 for a list of error messages that apply to all commands. See “ldapcfg command” on page 201 for information about command syntax and examples of command use.

Table 120. 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.

Table 120. *Idapcfg* command errors (continued)

Error message	Definition
Invalid option argument for <i>-option:argument</i> . <i>format</i> where: <ul style="list-style-type: none"> <li><i>option</i> identifies the option</li> <li><i>argument</i> identifies the invalid argument</li> <li><i>format</i> identifies the format of argument</li> </ul>	A user tries to issue a command with invalid arguments for the options which do not conform to the format specified.
Option argument for <i>-option</i> exceeds max length ( <i>maximum</i> characters): <i>argument</i> <ul style="list-style-type: none"> <li><i>option</i> identifies the option</li> <li><i>maximum</i> identifies the maximum allowed number of characters</li> <li><i>argument</i> identifies the argument</li> </ul>	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 385 for a list of error messages that apply to all commands. See “led command ” on page 211 for information about command syntax and examples of command use.

Table 121. *led* command errors

Error message	Definition
'blink' is not supported on blade[ <i>node_number</i> ] where <i>node_number</i> 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[ <i>node_number</i> ] where <i>node_number</i> identifies the compute node.	An error occurs while setting identify LED for the targeted compute node.
Error setting -loc for switch[ <i>number</i> ] where <i>number</i> 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 385 for a list of error messages that apply to all commands. See “list command” on page 214 for information about command syntax and examples of command use.

Table 122. 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 385 for a list of error messages that apply to all commands. See “monalerts command” on page 215 for information about command syntax and examples of command use.

Table 123. 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 385 for a list of error messages that apply to all commands. See “ntp command” on page 224 for information about command syntax and examples of command use.

Table 124. 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 <i>slot</i> where <i>slot</i> 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.

---

## permggroups command errors

This topic lists errors for the permggroups command.

See “Common errors” on page 385 for a list of error messages that apply to all commands. See “permggroups command” on page 228 for information about command syntax and examples of command use.

Table 125. permggroups 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 <b>Note:</b> 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 <b>Note:</b> 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 <i>group_name</i> cannot be deleted where <i>group_name</i> is the group name that was entered.	A user tries to delete the default permission group.
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 <b>Note:</b> 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 <b>Note:</b> 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): <i>number</i> where <i>number</i> 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: <i>number</i> where <i>number</i> is the device number that is not valid.	A user tries to specify RBS authority levels without specifying a valid device scope.

Table 125. *permggroups* command errors (continued)

Error message	Definition
Invalid rbs device (must be same device): <i>device</i> where <i>device</i> is the device that is not valid.	A user tries to specify RBS authority levels without specifying a valid device scope.
Invalid rbs device: <i>device</i> where <i>device</i> 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: <i>role</i> where <i>role</i> 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 <b>Note:</b> 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 <i>group_name</i> is in use and it cannot be deleted where <i>group_name</i> 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 385 for a list of error messages that apply to all commands. See “ping command” on page 232 for information about command syntax and examples of command use.

Table 126. *ping* command errors

Error message	Definition
Error reading network configuration	An error occurs while the CMM is reading the network configuration.
Index <i>index</i> IP address not found where the <i>index</i> 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 <i>ip_address</i> not found where the <i>ip_address</i> 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.



Table 126. ping command errors (continued)

Error message	Definition
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.

## mpolicy command errors

This topic lists errors for the mpolicy command.

See “Common errors” on page 385 for a list of error messages that apply to all commands. See “mpolicy command” on page 235 for information about command syntax and examples of command use.

Table 127. mpolicy 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 385 for a list of error messages that apply to all commands. See “portcfg command” on page 237 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 385 for a list of error messages that apply to all commands. See “ports command” on page 240 for information about command syntax and examples of command use.

Table 128. 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.

Table 128. ports command errors (continued)

Error message	Definition
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. <b>Note:</b> 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 <i>number</i> info where <i>number</i> is the port number that was entered.	An error occurs while reading port number information. <b>Note:</b> 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. <b>Note:</b> 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.
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. <b>Note:</b> This error message applies to only the I/O module target.
Maximum connections can not exceed <i>max</i> where <i>max</i> is the maximum number of allowed connections.	A user attempts to configure more than the maximum number of allowed connections. <b>Note:</b> 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. <b>Note:</b> This error message applies to only the I/O module target.

Table 128. ports command errors (continued)

Error message	Definition
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. <b>Note:</b> 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. <b>Note:</b> 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. <b>Note:</b> This error message applies to only the I/O module target.
Validating port failed	An error occurs while validating a port. <b>Note:</b> 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 385 for a list of error messages that apply to all commands. See “power command” on page 254 for information about command syntax and examples of command use.

Table 129. 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] 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.

Table 129. power command errors (continued)

Error message	Definition
-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] 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] 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] 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] 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 where slot is the I/O-module subslot.	An error occurs while retrieving a power state.
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 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.

Table 129. power command errors (continued)

Error message	Definition
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] where <i>x</i> 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 <i>min</i> and <i>max</i> where <i>min</i> and <i>max</i> 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 385 for a list of error messages that apply to all commands. See “pwrprofile command” on page 260 for information about command syntax and examples of command use.

Table 130. 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: <i>error</i> where <i>error</i> is: <ul style="list-style-type: none"> <li>• The group with the name already existed</li> <li>• Max group definitions reached</li> <li>• The group not found</li> <li>• Invalid parameters</li> <li>• Internal error</li> </ul>	An error occurs while the CMM is adding, deleting, or modifying a group.
Adding/deleting/modifying power schedule failed: <i>error</i> where <i>error</i> is: <ul style="list-style-type: none"> <li>• Max power schedules for this target group reached</li> <li>• Max power schedules reached</li> <li>• The power schedule not found</li> <li>• The group not found</li> <li>• Invalid parameters</li> <li>• Internal error</li> </ul>	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.

Table 130. *pwrprofile* command errors (continued)

Error message	Definition
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: <i>error</i> where <i>error</i> is specific information about the error.	An error occurs while the CMM is getting group information.
Getting schedule information of group <i>group_index</i> failed: <i>error</i> where: <ul style="list-style-type: none"> <li><i>group_index</i> is the group index specified.</li> <li><i>error</i> is specific information about the error.</li> </ul>	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 <i>key</i> ' where <i>key</i> 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: <i>index</i> . where <i>index</i> is the index specified.	A user tries to specify a non-numeric index.
Invalid group/power schedule index: <i>index</i> . It is out of range of 1 - <i>max</i> where: <ul style="list-style-type: none"> <li><i>index</i> is the index specified.</li> <li><i>max</i> is the highest index number that can be specified.</li> </ul>	A user tries to specify an index that is out of range.
Invalid group/power schedule index. Maximum value is <i>max</i> where <i>max</i> is the highest index number that can be specified.	A user tries to specify an index that is out of range.
Invalid group index: <i>group_index</i> where <i>group_index</i> 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: <i>group_name</i> . Consecutive dots not allowed where <i>group_name</i> is the group name specified.	A user tries to enter an invalid group name.
Invalid option argument for -n: <i>group_name</i> . Only alphanumeric characters and '.', or '_' allowed where <i>group_name</i> is the group name specified.	A user tries to enter an invalid group name.
Invalid syntax for group index: <i>group_index</i> where <i>group_index</i> 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.

Table 130. *pwrprofile* command errors (continued)

Error message	Definition
Invalid year. it must be between <i>min</i> - <i>max</i> where <i>min</i> and <i>max</i> 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 <i>max</i> where <i>max</i> 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 <i>max</i> characters where <i>max</i> 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 <i>max</i> characters where <i>max</i> 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 <i>max</i> characters where <i>max</i> 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 <i>max</i> chars where <i>max</i> is the highest number of characters that can be used.	A user tries to specify a bay string with too many characters.
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 385 for a list of error messages that apply to all commands. See “read command” on page 269 for information about command syntax and examples of command use.

Table 131. 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: <i>log_filename</i> where <i>log_filename</i> 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. <i>error_string</i> . where <i>error_string</i> 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 Flex System Enterprise 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): <i>passphrase</i> where <i>passphrase</i> 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.
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 385 for a list of error messages that apply to all commands. See “remotechassis command” on page 273 for information about command syntax and examples of command use.



Table 132. 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 Flex System Enterprise Chassiss 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 385 for a list of error messages that apply to all commands. See “reset command” on page 277 for information about command syntax and examples of command use.

Table 133. reset command errors

Error message	Definition
-exd not supported on switch[bay] 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] 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.
-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] 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.

Table 133. reset command errors (continued)

Error message	Definition
Power Operations not supported on blade[x]	A user tries to issue the <code>reset -T blade[x] -sft</code> 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 <i>node_number</i> with NMI not supported. where the <i>node_number</i> identifies the compute node.	A user tries to reset a compute node that does not support non-maskable interrupts (NMI).
Resetting blade <i>node_number</i> with NMI failed. where the <i>node_number</i> 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] 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] 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 <code>reset -o</code> override option.
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 <code>reset -o</code> 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.

Table 133. *reset command errors (continued)*

Error message	Definition
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 <code>reset -o</code> 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 385 for a list of error messages that apply to all commands. See “`scale` command” on page 279 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 385 for a list of error messages that apply to all commands. See “`sddump` command” on page 284 for information about command syntax and examples of command use.

Table 134. *sddump command errors*

Error message	Definition
Data dump collection of <i>type</i> type is not supported on blade <i>x</i> where <i>type</i> is the type of data requested and <i>x</i> is the number of the node bay.	The specified data collection type 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[ <i>x</i> ] where <i>x</i> is the I/O-module bay number.	An error occurs during data collection.
Error reading data dump status	An error occurs during data collection.
Error reading error string	An error occurs during data collection.
Initiate data collection of <i>type</i> type not supported on blade[ <i>x</i> ] where <i>type</i> is the type of data requested and <i>x</i> 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[ <i>x</i> ] where <i>x</i> 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 the compute 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 385 for a list of error messages that apply to all commands. See “sdemail command” on page 286 for information about command syntax and examples of command use.

Table 135. 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 385 for a list of error messages that apply to all commands. See “security command” on page 287 for information about command syntax and examples of command use.

Table 136. 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 385 for a list of error messages that apply to all commands. See “service command” on page 290 for information about command syntax and examples of command use.

Table 137. 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.

Table 137. service command errors (continued)

Error message	Definition
Invalid option for this target: - <i>option</i> where <i>option</i> 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 reset (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 reset (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 reset (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 reset (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 reset (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 385 for a list of error messages that apply to all commands. See “smtp command” on page 293 for information about command syntax and examples of command use.

Table 138. 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 385 for a list of error messages that apply to all commands. See “snmp command” on page 295 for information about command syntax and examples of command use.

Table 139. 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.
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 385 for a list of error messages that apply to all commands. See “sol command” on page 308 for information about command syntax and examples of command use.

Table 140. 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.

Table 140. sol command errors (continued)

<b>Error message</b>	<b>Definition</b>
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.
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] 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.

---

## ssshcfg command errors

This topic lists errors for the ssshcfg command.

See “Common errors” on page 385 for a list of error messages that apply to all commands. See “ssshcfg command” on page 315 for information about command syntax and examples of command use.

Table 141. ssshcfg 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.

---

## ssslcfg command errors

This topic lists errors for the ssslcfg command.

See “Common errors” on page 385 for a list of error messages that apply to all commands. See “ssslcfg command” on page 317 for information about command syntax and examples of command use.

Table 142. ssslcfg command errors

Error message	Definition
-csa can only be used with -gen ca	A user tries to issue the -csa option without the -gen option or without providing the ca 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 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.
-u must be provided to import a trusted certificate	A user tries to issue an import trusted certificate command without the -u option.



Table 142. *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: <i>node</i> where <i>node</i> 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 <i>-csa</i> .
Cannot open file: <i>filename</i> where <i>filename</i> 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 = <i>error</i> where <i>error</i> specifies error.	An error occurs while the CMM is mapping the file to memory.
CMM security policy disallows <i>-httpse disable</i> ( <i>http enable</i> ) 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 <i>trusted_certindex</i> failed where <i>index</i> is the number of the selected trusted certificate, between 1 and 4 (inclusive).	A user tries to delete a nonexistent trusted certificate.
Downloading <i>Cert/CA/CSR</i> to <i>argument</i> failed where: <ul style="list-style-type: none"> <li><i>Cert/CA/CSR</i> specifies whether the user tried to download a certificate, certificate authority, or certificate signing request.</li> <li><i>argument</i> identifies the remote location of the item be downloaded from. It must specify a fully qualified filename.</li> </ul>	An error occurs while the CMM is downloading a certificate, certificate authority, or certificate signing request.
Error: unknown certificate	An error occurs because an unknown certificate type is referred to.
Exporting <i>Cert/CSR/CA</i> failed where <i>Cert/CSR/CA</i> 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.
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.
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.

Table 142. *sslcfg* command errors (continued)

Error message	Definition
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 <i>url</i> failed where <i>url</i> 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 Trusted certificate: server	A user tries to issue a command for a trusted certificate with a target of server'.
Invalid URL for -u: <i>url</i> where <i>url</i> is the URL that was entered.	A user tries to enter a URL that is not valid.
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 <i>Cert/CSR/CA</i> available. where <i>Cert/CSR/CA</i> 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_ <i>certindex</i> available. where <i>index</i> 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.
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.
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 CA failed	An error occurs while viewing a certificate authority.
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 385 for a list of error messages that apply to all commands. See “syslog command” on page 328 for information about command syntax and examples of command use.

Table 143. *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 385 for a list of error messages that apply to all commands. See “tcpcmdmode command” on page 333 for information about command syntax and examples of command use.

Table 144. *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, <code>tcpcmdmode -t200m</code> .
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 <i>maximum</i> where <i>maximum</i> 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 <i>maximum</i> where <i>maximum</i> 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 385 for a list of error messages that apply to all commands. See “temps command” on page 336 for information about command syntax and examples of command use.

Table 145. temps command errors

Error message	Definition
Error getting temperature data from target	An error occurs while retrieving temperature data.
Getting power state of blade <i>node_number</i> failed. where <i>node_number</i> 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 385 for a list of error messages that apply to all commands. See “trespass command” on page 337 for information about command syntax and examples of command use.

Table 146. 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 <i>-twe enabled</i> 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 385 for a list of error messages that apply to all commands. See “uicfg command” on page 339 for information about command syntax and examples of command use.

Table 147. 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.

Table 147. uicfg command errors (continued)

Error message	Definition
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.
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: <ul style="list-style-type: none"> <li>• A community is configured without an IP address or host name.</li> <li>• A duplicate community name is configured.</li> <li>• At least one configured community is required to enable SNMPv1.</li> <li>• IP address of 0.0.0.0 is allowed only for the first host name in the first community.</li> <li>• IP address of 0.0.0.0 is allowed only when the first community is configured as GET or SET access type.</li> <li>• System contact must be defined to enable SNMPv1/v3.</li> <li>• System location must be defined to enable SNMPv1/v3.</li> </ul>
Error sanity checking of SNMP configuration.	An error occurs while the CMM is sanity-checking the SNMP configuration.
Maximum connections can not exceed <i>maximum</i> where <i>maximum</i> 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 <i>maximum</i> where <i>maximum</i> 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 385 for a list of error messages that apply to all commands. See “update command” on page 343 for information about command syntax and examples of command use.

Table 148. 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.

Table 148. update command errors (continued)

Error message	Definition
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.
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 <i>index</i> . <i>maximum</i> where <i>index</i> 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 <i>percentage</i> where the <i>percentage</i> 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 <i>percentage</i> . where the <i>percentage</i> value varies based on when the problem was encountered.	An error occurs during the flash firmware update.
Flash preparation - error sending packet file <i>filename</i> . where <i>filename</i> identifies the file being updated.	An error occurs during the flash firmware update.
Flash preparation error. Packet percent complete <i>percentage</i> . Flash percent complete <i>percentage</i> . where the <i>percentage</i> 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 <i>percentage</i> . where the <i>percentage</i> 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 <i>bay_number</i> failed. where the <i>bay_number</i> 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 <i>maximum</i> where <i>maximum</i> designates the largest permitted index value.	A user tries to enter an image index that is greater than the maximum permitted index value.

Table 148. update command errors (continued)

Error message	Definition
Invalid option.	<p>An invalid command option is entered. For the update command, invalid command option errors include:</p> <ul style="list-style-type: none"> <li>• the -i (IP address) command option does not have an IP address parameter</li> <li>• the -i (IP address) command option specifies an invalid IP address</li> <li>• attempting to enter the -i (IP address) command option without the -n (filename) command option</li> <li>• the -n (filename) command option does not have a file name parameter</li> <li>• attempting to enter the -n (filename) command option without the -i (IP address) command option</li> <li>• attempting to enter the -v (verbose) command option without the -i (IP address) command option and -n (filename) command option</li> <li>• attempting to enter the -v (verbose) command option with the -a command option</li> </ul>
Invalid syntax.	The user tries to execute a command without specifying a command option.
CMMbay_number is not installed. 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.
<p>TFTP Error: error_code. where the error_code can have one of the following values:</p> <ul style="list-style-type: none"> <li>• Access violation.</li> <li>• Connection failure.</li> <li>• Disk full or allocation exceeded.</li> <li>• File already exists.</li> <li>• File error.</li> <li>• File not found.</li> <li>• Illegal option negotiation.</li> <li>• Illegal TFTP operation.</li> <li>• Unable to allocate memory.</li> <li>• Unknown transfer ID.</li> <li>• Unknown user.</li> </ul>	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 148. 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 <i>bay_numbername</i> , where the <i>bay_number</i> and <i>name</i> 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 <i>bay_numbername</i> , where the <i>bay_number</i> and <i>name</i> 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 <i>bay_numbername</i> , where the <i>bay_number</i> and <i>name</i> 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 <i>node_numbername</i> , where the <i>node_number</i> and <i>name</i> 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 385 for a list of error messages that apply to all commands. See “uplink command” on page 349 for information about command syntax and examples of command use.

Table 149. 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. <b>Note:</b> 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 149. 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. <b>Note:</b> 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, <code>uplink -- del0</code> .
No option argument for <i>option</i> where <i>option</i> 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 <i>option</i> is out of the valid range (between 1 and 2880 minutes). where <i>option</i> is the number of minutes specified.	The user input for an option is out of the range.
The option argument for <i>option</i> is out of the valid range (between 10 and 172800 seconds). where <i>option</i> 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 385 for a list of error messages that apply to all commands. See “users command” on page 353 for information about command syntax and examples of command use.

Table 150. 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 150. 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 <b>Note:</b> 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 <b>Note:</b> 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 <i>user</i> failed where <i>user</i> is the user name specified by the user <b>Note:</b> 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. <b>Note:</b> 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 <b>Note:</b> 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 <i>URL</i> failed where <i>URL</i> is the URL specified by the user	An error occurs when the user tries to download to a specified URL.
Duplicate group name: <i>group_name</i> where <i>group_name</i> is the group name specified by the user	A user tries to create a group name that already exists.

Table 150. users command errors (continued)

Error message	Definition
<p>Enable a user failed</p> <p><b>Note:</b> This error message might include additional information that provides details about the error, if this additional information is provided by the process or device.</p>	<p>An error occurs while the CMM is enabling a user.</p>
<p>Error writing data for option -ipmismmpv3</p> <p><b>Note:</b> This error message might include additional information which provides details about the error and corrective actions.</p>	<p>An error occurs while the CMM is writing IPMIv3 information for the indicated user.</p> <p><b>Example:</b></p> <pre>system&gt; users -T mm[2] -n test -ipmismmpv3 enabled</pre> <p><b>Error writing data for option -ipmismmpv3</b></p> <p><b>User test: account is locked, password must be changed.</b></p> <p><b>system&gt;</b></p> <p>This indicates that the test user account is locked and that its password needs to be changed.</p>
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.
<p>Getting user information failed</p> <p><b>Note:</b> This error message might include additional information that provides details about the error, if this additional information is provided by the process or device.</p>	An error occurs while the CMM is getting user information.
<p>Getting user names failed</p> <p><b>Note:</b> This error message might include additional information that provides details about the error, if this additional information is provided by the process or device.</p>	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.
<p>Group <i>group_name</i> not found</p> <p>where <i>group_name</i> is the group name specified by the user</p>	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 150. users command errors (continued)

Error message	Definition
<p>Modifying user failed  <b>Note:</b> This error message might include additional information that provides details about the error, if this additional information is provided by the process or device.</p>	An error occurs while the CMM is modifying a user.
<p>Modifying user password failed  <b>Note:</b> This error message might include additional information that provides details about the error, if this additional information is provided by the process or device.</p>	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 <i>key_index</i> found for user: <i>user_name</i> where <i>key_index</i> is the is a user profile index key and <i>user_name</i> 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.
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 <i>maximum</i> where <i>maximum</i> 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 <i>group_name</i> exceeds max of <i>maximum</i> where <i>group_name</i> is the is group name entered and <i>maximum</i> 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.
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 <i>maximum</i> where <i>maximum</i> is the maximum number of groups specified by the user	A user tries to set up too many groups.

Table 150. users command errors (continued)

Error message	Definition
The user name cannot be longer than <i>maximum</i> characters for SNMPv3/IPMI provisioning. where <i>maximum</i> 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 <b>Note:</b> 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 <b>Note:</b> 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.

## vlan command errors

This topic lists error messages for the vlan command.

See “Common errors” on page 385 for a list of error messages that apply to all commands. See “vlan command” on page 371 for information about command syntax and examples of command use.

Table 151. 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 <i>time</i> minutes using -commit. where <i>time</i> 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.

Table 151. vlan command errors (continued)

Error message	Definition
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.
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.

Table 151. vlan command errors (continued)

Error message	Definition
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.
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 385 for a list of error messages that apply to all commands. See “volts command” on page 382 for information about command syntax and examples of command use.

Table 152. volts command errors

Error message	Definition
Error getting voltage data from target	An error occurs while retrieving voltage data.
Getting power state of blade <i>node_number</i> failed. where <i>node_number</i> 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 385 for a list of error messages that apply to all commands. See “write command” on page 383 for information about command syntax and examples of command use.

Table 153. 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. <i>error_string</i> . where <i>error_string</i> is specific information about the error.	The CMM is unable to transfer the file.
Firmware update is in progress. Try again later.	A user tries to save the CMM configuration to the Flex System Enterprise 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): <i>passphrase</i> where <i>passphrase</i> 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.

Table 153. write command errors (continued)

<b>Error message</b>	<b>Definition</b>
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](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 DSA data

You can use the Enhanced Customer Data Repository to send diagnostic data to IBM.

Before you send diagnostic data to IBM, read the terms of use at <http://www.ibm.com/de/support/ecurep/terms.html>.

You can use any of the following methods to send diagnostic data:

- **Standard upload:**  
[http://www.ibm.com/de/support/ecurep/send\\_http.html](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](http://www.ecurep.ibm.com/app/upload_hw)
- **Secure upload:**  
[http://www.ibm.com/de/support/ecurep/send\\_http.html#secure](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](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 IBM Taiwan product service.

台灣 IBM 產品服務聯絡方式：  
台灣國際商業機器股份有限公司  
台北市松仁路 7 號 3 樓  
電話：0800-016-888

IBM Taiwan product service contact information:

IBM Taiwan Corporation  
3F, No 7, Song Ren Rd.  
Taipei, Taiwan  
Telephone: 0800-016-888



---

## 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>



---

## 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 154. Limits for particulates and gases

Contaminant	Limits
Particulate	<ul style="list-style-type: none"><li>• The room air must be continuously filtered with 40% atmospheric dust spot efficiency (MERV 9) according to ASHRAE Standard 52.2<sup>1</sup>.</li><li>• 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.</li><li>• The deliquescent relative humidity of the particulate contamination must be more than 60%<sup>2</sup>.</li><li>• The room must be free of conductive contamination such as zinc whiskers.</li></ul>
Gaseous	<ul style="list-style-type: none"><li>• Copper: Class G1 as per ANSI/ISA 71.04-1985<sup>3</sup></li><li>• Silver: Corrosion rate of less than 300 in 30 days</li></ul>
<p><sup>1</sup> ASHRAE 52.2-2008 - <i>Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size</i>. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.</p> <p><sup>2</sup> 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.</p> <p><sup>3</sup> ANSI/ISA-71.04-1985. <i>Environmental conditions for process measurement and control systems: Airborne contaminants</i>. Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.</p>	

---

## 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 2004/108/EC 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 Information Technology Equipment according to European Standard EN 55022. 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

## 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 2004/108/EG (früher 89/336/EWG) zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbchern 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 Betriebsmitteln**

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 2004/108/EG (früher 89/336/EWG) 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 EG Richtlinie 2004/108/EC (früher 89/336/EWG), für Geräte der Klasse A.**

Dieses Gerät ist berechtigt, in bereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen. Verantwortlich für die Konformitätserklärung nach Paragraph 5 des EMVG ist die Lenovo (Deutschland) GmbH, Gropiusplatz 10, D-70563 Stuttgart.

Informationen in Hinsicht EMVG Paragraph 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 Funkstrungen 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 entstrahlt 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 Strungen 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 Handbchern angegeben, zu installieren und zu betreiben.

## **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妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

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.

## Korea Communications Commission (KCC) statement

이 기기는 업무용(A급)으로 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 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 классу А. В жилых помещениях оно может создавать радиопомехи, для снижения которых необходимы дополнительные меры

## 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。

---

# Index

## A

- accessibility features for the CMM 2
- account inactivity alert time
  - set for CMM 40
- account inactivity disable time
  - set for CMM 41
- account lockout period
  - set for CMM 42
- account security commands 35
- account security settings
  - display for CMM 36
  - enable complex password for CMM user authentication 39
  - enable default administration password expiration for CMM 40
  - enable password change at first login to CMM 42
  - set CMM account inactivity alert time 40
  - set CMM account inactivity disable time 41
  - set CMM account lockout period 42
  - set CMM authentication logging timeout 38
  - set CMM CLI inactivity timeout 39
  - set CMM default to high 37
  - set CMM default to legacy 36
  - set CMM maximum LDAP sessions for user 42
  - set CMM maximum number of login failures 41
  - set CMM minimum number of different characters for password 40
  - set CMM password expiration time 43
  - set CMM password minimum change interval 43
  - set CMM password reuse cycle 44
  - set CMM user authentication method 39
  - set CMM web interface inactivity timeout 44
- accsecfg 36
  - options
    - alt 38
    - am 39
    - cp 39
    - ct 39
    - dc 40
    - de, on 40
    - high 37
    - ia 40
    - ici 41
    - id 41
    - legacy 36
    - lf 41
    - lp 42
    - mls 42
    - pc, on 42
    - pe 43
    - pi 43
    - rc 44
    - wt 44
- accsecfg command errors 387
- accsecfg commands 35
  - example 44
- accumulate timeout
  - set for SOL 311
- acknowledge call-home activity log entry
  - CMM 78
- acoustic mode, disable 144
- acoustic mode, enable 144
- activate firmware
  - I/O module 348
  - switch 348
- Active Directory group, add 152
- Active Directory group, delete 155
- Active Directory group, set authority level 153
- Active Directory groups, display (all) 151
  - Active Directory groups, display (specific) 151
  - add Active Directory group 152
  - add Call Home events
    - CMM 132
  - add power group 262
  - add power schedule 263
  - add SSH user public key 361
  - add user 357
  - add user permission group 229
  - add-in card
    - command target 126
  - address
    - IPv6 initial connection 18
    - link local 18
  - address prefix length
    - set for channel 0 of CMM 176
    - set for compute node 183
    - set for I/O module 190
  - advanced failover settings
    - disable network interface for standby CMM 46
    - display for CMM 46
    - enable network interface for standby CMM and allow IP swap during failover 46
    - enable network interface for standby CMM and prevent IP swap during failover 46
  - advfailover 46
    - options
      - ip.noswap 46
      - ip.off 46
      - ip.swap 46
  - advfailover command 45
    - example 47
  - advfailover command errors 389
  - air filter
    - set notification interval 47
    - view notification interval 47
  - air filter notification 47
  - air flow trending, display (chassis) 143
  - airfilter 47
    - CMM 47
    - options
      - freq 47
  - airfilter command
    - 0, 1, 3, 6 months 47
    - notification interval 47
  - airfilter command errors 389
  - alarm panel
    - command target 126
  - alert
    - test 56
  - alert categories (enhanced legacy)
    - disable 216
    - enable 216
  - alert notification method, set 55
  - alert recipient, create 51
  - alert recipient, delete 51
  - alert recipient, set email address 55
  - alert recipient, set name 53
  - alert recipient, set status 53
  - alert recipients, manage 50
  - alert state
    - display all 216
  - alert type, filter 54
  - alert type, set 54
  - alercfg 48
    - options
      - dr 48
      - rl 48-49
      - si 49

- alertcfg command errors 389
- alertcfg commands 48
  - example 49
- alertentries 50
  - options
    - 1 through 12 50
    - create (n, status, f, t, e, i) 51
    - del 51
    - e 55
    - f 54
    - n 53
    - status 53
    - t 55
    - test 56
- alertentries command 50
- alertentries command errors 389
- alertentries commands
  - example 56
- alerts
  - disable monitoring for all critical 216
  - disable monitoring for all informational 220
  - disable monitoring for all warning 218
  - disable monitoring for chassis critical 217
  - disable monitoring for chassis informational 221
  - disable monitoring for chassis warning 219
  - disable monitoring for cooling device critical 217
  - disable monitoring for cooling device informational 224
  - disable monitoring for cooling device warning 220
  - disable monitoring for event log informational 222
  - disable monitoring for event log warning 219
  - disable monitoring for inventory change informational 222
  - disable monitoring for I/O module critical 217
  - disable monitoring for I/O module informational 221
  - disable monitoring for I/O module warning 219
  - disable monitoring for network change informational 223
  - disable monitoring for node device critical 216
  - disable monitoring for node device informational 221
  - disable monitoring for node device warning 218
  - disable monitoring for power state informational 222
  - disable monitoring for power supply critical 218
  - disable monitoring for power supply informational 224
  - disable monitoring for power supply warning 220
  - disable monitoring for system management critical 217
  - disable monitoring for system management
    - informational 221
  - disable monitoring for system management warning 219
  - disable monitoring for user activity informational 223
  - display all states 216
  - enable monitoring for all critical 216
  - enable monitoring for all informational 220
  - enable monitoring for all warning 218
  - enable monitoring for chassis critical 217
  - enable monitoring for chassis informational 221
  - enable monitoring for chassis warning 219
  - enable monitoring for cooling device critical 217
  - enable monitoring for cooling device informational 224
  - enable monitoring for cooling device warning 220
  - enable monitoring for event log informational 222
  - enable monitoring for event log warning 219
  - enable monitoring for inventory change informational 222
  - enable monitoring for I/O module critical 217
  - enable monitoring for I/O module informational 221
  - enable monitoring for I/O module warning 219
  - enable monitoring for network change informational 223
  - enable monitoring for node device critical 216
  - enable monitoring for node device informational 221
  - enable monitoring for node device warning 218
  - enable monitoring for power state informational 222
  - enable monitoring for power supply critical 218
  - enable monitoring for power supply informational 224
  - enable monitoring for power supply warning 220
  - enable monitoring for system management critical 217
  - enable monitoring for system management
    - informational 221
  - enable monitoring for system management warning 219
- enable monitoring for user activity informational 223
- exclude service information with email alerts 49
- include service information with email alerts 49
- alerts, display 158
  - timestamp 159
- algorithms, encryption 17
- apply IPv4 configuration changes
  - CMM 167
- assign power schedule to power group 263
- assistance, getting 461
- Attention notice, meaning 2
- attributes, display for firmware 344
- Australia Class A statement 468
- authentication (mutual) of CSR import
  - using CLI 31
- authentication (non-mutual) of LDAP certificate import
  - using CLI 30
- authentication logging timeout
  - set for CMM 38
- authentication method
  - LDAP 209
- authentication of CA
  - using CLI 28
  - using web interface 28
- authentication of certificate
  - using CLI 28
  - using web interface 28
- authentication of CSR
  - using CLI 28
  - using web interface 28
- authority, command 10
- autoftp
  - options
    - desc 58
    - i 58
    - m 58
    - p 58
    - pw 58
    - u 58
- autoftp command errors 390
- autoftp commands 57
  - example 59
- autoftp settings
  - call-home 58
- automatic power-on policy
  - set for compute node 258

## B

- backup
  - configuration 383
  - permission groups 383
  - users 383
- baud rate
  - set for serial port of CMM 238
- bay data
  - clear bay data 61
  - clear bay data for specific bay 61
  - compute node 60
  - display bay data 60
  - display bay data for specific bay 60
  - set bay data 62
  - set data definition to specific compute node 63
- baydata 60
  - options
    - b bay\_num 60
    - b bay\_num -clear 61
    - b bay\_num -data "data\_definition" 63
    - clear 61
    - data "data\_definition" 62
- baydata command errors 391
- baydata commands 59
  - example 64

- binding method
  - LDAP 209
- blink identify LED 213
- BMC
  - command target 126
- boot device
  - clear IP address 67
  - display information 66
  - set IP address 67
- boot mode
  - display for compute node 65
  - set for compute node 65
- boot sequence
  - display for compute node 66
  - set for compute node 66
- bootmode 65
  - options
    - p 65
- bootmode command errors 392, 431
- bootmode commands 64
  - example 65
- bootseq 66
  - options
    - g 67
    - i 67
    - id 66
    - s 67
  - seq 66
- bootseq command errors 392
- bootseq commands 66
  - example 67

## C

- CA authentication
  - using CLI 28
  - using web interface 28
- CA import (mutual authentication)
  - using CLI 31
- CA import (non-mutual authentication)
  - using CLI 30
- CA self-signed root certificate
  - download certificate file 321
- call-home
  - autoftp settings 58
  - problem description 80
  - test call home 80
- call-home activity log
  - acknowledge call-home activity log entry for CMM 78
  - display for CMM 77
  - display FTP/TFTP server entries for CMM 77
  - display Lenovo Support entries for CMM 78
  - unacknowledge call-home activity log entry for CMM 78
- Canada Class A electronic emission statement 468
- Caution notice, meaning 2
- centralized account management
  - disable 137
- centralized user account management
  - disable 138
  - disable IPMI/SNMPv3 for CMM 367
  - disable IPMI/SNMPv3 for compute nodes 366
  - enable IPMI/SNMPv3 for CMM 367
  - enable IPMI/SNMPv3 for compute nodes 366
- certificate
  - import 327
  - upload 327
- certificate (SSL)
  - download certificate file (format) 322
- certificate authentication
  - using CLI 28
  - using web interface 28
- certificate authority
  - generate self-signed certificate 319
- certificate file (CA self-signed root certificate)
  - download 321
- certificate file (SSL certificate) (format)
  - download 322
- certificate file (SSL CSR) (format)
  - download 322
- certificate import (mutual authentication)
  - using CLI 31
- certificate import (non-mutual authentication)
  - using CLI 30
- change command environment 35, 124
- change user password (other user) 359
- change user password (own password) 358
- change user permission group 230
- chassis
  - enable power capping 146
  - enable power management 146
  - set hot air recirculation threshold 143
  - set name 96
  - set rack location 97
  - set rack unit location 98
  - set room location 98
  - set static power limit 144
- Chassis CMM
  - snmp commands 295
- chassis internal network command
  - cin 84
- chassis internal network configuration 84
- chassis internal network status 90
- chassis internal network status command 90
- chassis module
  - display activity 136
- chassis module activity
  - display 136
- chassis security policy 289
  - display CMM setting 289
- chassis, display air flow trending 143
- chassis, display exhaustive heat trending information 142
- chassis, hot air recirculation detection state, set 143
- chconfig 70
  - options
    - ace 73
    - acph 73
    - acphe 73
    - ca 71, 73
    - can 73
    - cci 71, 73
    - ce 71
    - cn 71
    - co 71
    - cph 71
    - cphe 71
    - cs 71, 73
    - cz 71, 73
    - li 70
    - loc 75
    - mlph 71, 73
    - po 75
    - ps 75
    - pw 75
    - sa 71
    - sc 71, 73
    - u 75
- chconfig command errors 393
- chconfig commands 69
  - example 75
- China Class A electronic emission statement 470
- chlog 77
  - options
    - ack 78
    - f 77
    - s 78
- chlog command errors 395
- chlog commands 76
  - example 78

- chmanual
  - options
    - desc 80
    - test 80
- chmanual command errors 396
- chmanual commands 79
  - example 80
- CIM
  - disable for CMM 248, 340
  - enable for CMM 248, 340
- CIM port number
  - set for CMM 244
- CIM subscription 81
  - clear 82
  - display destination 82
  - display status 82
- cimsub 82
- cimsub command 81
- cimsub command errors 396
- cimsub commands
  - example 82
- cin 85
  - options
    - entry\_index -ip ip\_address 88
    - entry\_index clear 86
    - entry\_index en 87
    - entry\_index id 87
    - global en 85
    - id 88
    - vlan\_id -ip ip\_address 87
- CIN
  - turn all index entries on or off 86
- cin all
  - options
    - clear 85
    - en state 86
- cin command
  - chassis internal network 84
- cin command errors 397
- cin commands
  - example 89
- cin configuration
  - Specify VLAN ID 88
- CIN configuration 86
- CIN configuration entries 85
- CIN configuration entry
  - create 87
  - delete 86
  - disable 87
  - enable 87
  - Specify IP address 88
- CIN configuration table
  - display for CMM 85
- CIN index entry
  - create 87
  - Specify IP address 88
- CIN state
  - set for enable or disable 85
- CIN status table entries 90
- cinstatus 90
- cinstatus command 90
- cinstatus command errors 398
- cinstatus commands
  - example 90
- cipher suite
  - set for CMM 104
- Class A electronic emission notice 468
- clear
  - CIM subscription 82
    - options
      - cnfg 92–93
      - cnfg, o 92
- clear CIN configuration
  - CMM 85
- clear CMM event log commands 93
  - example 94
- clear command 91
- clear command errors 398
- clear commands
  - example 93
- clear event log
  - CMM 94
- clear for CMM 85
- clearlog 94
  - I 94
- clearlog command errors 399
- clearlog commands 93
  - example 94
- CLI
  - CA authentication 28
  - CA mutual authentication import 31
  - CA non-mutual authentication import 30
  - certificate authentication 28
  - CSR authentication 28
  - CSR import (mutual authentication) 31
  - exit 133
  - exit codes for SSH 22
  - LDAP certificate import (non-mutual authentication) 30
  - mutual authentication certificate import 31
  - non-mutual authentication certificate import 30
- CLI configuration
  - CMM 24
  - Flex System Enterprise Chassis 23
- CLI inactivity timeout
  - set for CMM 39
- CLI key sequence
  - set for SOL 313
- CLI SFTP server
  - disable for CMM 316
  - enable for CMM 316
- CLI SSH server
  - disable for CMM 316
  - enable for CMM 316
- clock commands 106
  - example 108
- clock settings
  - display for CMM 106
  - display valid timezones 106
  - display valid timezones (verbose) 106
- CMM
  - account security commands 35
  - accseccfg 35
  - accseccfg commands 35, 44
  - acknowledge call-home activity log entry 78
  - add Active Directory group 152
  - add Call Home events 132
  - add power group 262
  - add power schedule 263
  - add SSH user public key 361
  - add user 357
  - add user permission group 229
  - advfailover command 45, 47
    - example 47
  - airfilter 47
  - assign power schedule to power group 263
  - autoftp commands 57, 59
  - bay data 60
  - cabling 14
  - change user password (other user) 359
  - change user password (own password) 358
  - change user permission group 230
  - chconfig commands 69, 75
  - chmanual commands 79–80
  - cimsub commands 81
  - cin commands 84
  - cinstatus commands 90
  - clear CIM subscription 82
  - clear CIN configuration entries 85
  - clear event log 94
  - clear event log commands



- example 94
- command target 125
- config command 95, 99
  - example 99
- configuring for CLI 24
- create alert recipient 51
- create user 357
- crypto command 103, 105
  - example 105
- default IP address 17
- delete Active Directory group 155
- delete alert recipient 51
- delete CIN configuration 86
- delete file 134
- delete power group 267
- delete power schedule 268
- delete user 356
- delete user permission group 231
- dhcpcinfo commands 108
- direct connection 15
- disable centralized user account management (IPMI/
  - SNMPv3) 367
- disable CIM 248, 340
- disable CIN configuration entry 87
- disable CLI SFTP server 316
- disable CLI SSH server 316
- disable command-line interface 340
- disable DHCPv6 177
- disable DNS 121
- disable FTP 247
- disable HTTPS port 248
- disable IPv6 stateless auto-configuration 177
- disable logical uplink failover 351
- disable network interface for standby 46
- disable NTP 248
- disable secure TCP command mode 250, 342
- disable SFTP 247
- disable SLP 248
- disable SNMP traps 249
- disable SNMPv1 341
- disable SNMPv1 agent 249
- disable SNMPv3 341
- disable SNMPv3 agent 249
- disable SSH port 249
- disable static IPv6 configuration 176
- disable TCP command mode 250, 341
- disable Telnet port 250
- disable TFTP 251
- disable user 355
- disable web interface 342
- display (reset counter) event log 113
- display account security settings 36
- display active users 354
- display advanced failover settings 46
- display alert properties (all recipients) 50
- display alert properties (single recipient) 50
- display all Active Directory groups 151
- display all event log entries 113
- display all event log filters 114
- display all power groups 261
- display all power schedules 261
- display all user permission groups 228
- display all users 354
- display call-home activity log 77
- display CIM subscription destination 82
- display CIM subscription status 82
- display CIN configuration table 85
- display clock settings 106
- display complete SSH public key 363
- display contact name 95
- display cryptographic settings 104
- display date 106
- display daylight-savings time setting 106
- display DNS configuration 120
- display DSA host key information 315

- display entries of CIN status table 90
- display event log 113
- display event log commands
  - example 117
- display event log entries filtered by date 114
- display event log entries filtered by severity level 115
- display event log entries filtered by source 115–116
- display events list 132
- display feature licenses 135
- display file list 134
- display free space 132, 134
- display FTP/TFTP server call-home activity log 77
- display global remote alert settings 48
- display GMT offset 106
- display LDAP settings 202
- display Lenovo Support call-home activity log 78
- display licenses 135
- display location 95
- display log entries with auxiliary data 114
- display log entries with call-home events 113
- display log entries with Event ID 113
- display log entries with log sequence number 113
- display name 95
- display network port settings 241
- display NTP configuration 225
- display open ports 241
- display power group 261
- display RSA host key information 315
- display serial port configuration 238
- display SFTP status 315
- display single user 355
- display SMTP server host name 294
- display SMTP server IP address 294
- display SNMP configuration 296
- display specific Active Directory groups 151
- display specific user permission group 228
- display SSH public key 363
- display SSH status 315
- display state of -lse option 116
- display status 118
- Display status of first five CIN entries 90
- display syslog configuration 329
- display temperature 336
- display time 106
- display trespass feature status 337
- display user interface settings 340
- dns commands 120, 123
  - example 123
- download SSH public key 363
- enable centralized user account management (IPMI/
  - SNMPv3) 367
- enable CIM 248, 340
- enable CIN configuration entry 87
- enable CLI SFTP server 316
- enable CLI SSH server 316
- enable command-line interface 340
- enable complex password 39
- enable default administration password expiration 40
- enable DHCPv6 configuration 177
- enable DNS 120
- enable dynamic DNS 121
- enable FTP 247
- enable HTTPS port 248
- enable IPv6 stateless auto-configuration 177
- enable logical uplink failover 351
- enable monitoring of event log state 117
- enable network interface for standby and allow IP swap 46
- enable network interface for standby and prevent IP
  - swap 46
- enable NTP 225, 248
- enable password change at first login 42
- enable physical uplink failover 350
- enable secure TCP command mode 250
- enable SFTP 247
- enable SLP 248

enable SNMP agent (SNMPv1) 296  
enable SNMP agent (SNMPv3) 296  
enable SNMP traps 249, 296  
enable SNMPv1 341  
enable SNMPv1 agent 249  
enable SNMPv3 341  
enable SNMPv3 agent 249  
enable SSH port 249  
enable static IPv6 configuration 176  
enable TCP command mode 250  
enable Telnet port 250  
enable TFTP 251  
enable trespass feature 337  
enable user 356  
enable V3 authentication for NTP 226  
enable web interface 342  
Ethernet network settings commands  
  example 191  
export SSH public key 363  
failover configuration 350  
filter alert type 54  
filter log entries by call-home events flag 116  
Flex System Manager software communication 333  
generate host key 316  
generate syslog test message 332  
ifconfig commands 164, 191  
import (add) SSH public key 362  
import (update) SSH public key 362  
IPv4 configuration changes 167  
ldapcfg command 201, 210  
  example 210  
logical uplink failover delay 351  
logical uplink failover IP address 352  
logical uplink failover IPv6 IP address 352  
modify power group 264  
modify power schedule 266  
modify user permission group 230  
network connection 15  
physical uplink failover delay 350  
portcfg commands 237, 239  
ports command 240, 253  
  example 253  
read CIN status table entries 90  
read command 269, 273  
  example 273  
remotechassis command 273, 275  
  example 275  
remove SSH user public key 361  
reset (failover) 278  
reset (primary with override) 277  
reset (primary) 277  
reset (standby) 278  
reset configuration (keep logs with override) 92  
reset configuration (keep logs) 92  
reset network port settings 242  
restore configuration from file 271  
restore configuration from file (verbose) 271  
restore configuration from file (verbose) and reset 273  
restore configuration from file and reset 272  
restore default configuration 91  
save configuration to file 384  
save event log 117  
sdemail commands 286–287  
security commands 35, 287, 289  
serial connection 16, 20  
serial port settings commands  
  example 239  
service commands 290  
set account inactivity alert time 40  
set account inactivity disable time 41  
set account lockout period 42  
set account security default to high 37  
set account security default to legacy 36  
set Active Directory group authority level 153  
set alert notification method 55  
set alert recipient email address 55  
set alert recipient name 53  
set alert recipient status 53  
set alert type 54  
set authentication logging timeout 38  
set chassis security policy 289  
set CIM port number 244  
set CIN state for global enable or disable 85  
set cipher suite 104  
set CLI inactivity timeout 39  
set contact name 99  
set cryptographic mode 104  
set cryptographic settings 104  
set date 107  
set DNS first IPv4 IP address 121  
set DNS first IPv6 IP address 122  
set DNS second IPv4 IP address 122  
set DNS second IPv6 IP address 123  
set DNS server priority 123  
set DNS third IPv4 IP address 122  
set DNS third IPv6 IP address 123  
set Ethernet channel 0 address prefix length 176  
set Ethernet channel 0 data rate 173  
set Ethernet channel 0 duplex mode 173  
set Ethernet channel 0 floating IP address (IPv4) 168  
set Ethernet channel 0 floating IP address (IPv6) 168  
set Ethernet channel 0 gateway IP address (IPv4) 170  
set Ethernet channel 0 gateway/default route (IPv6) 170  
set Ethernet channel 0 hostname 171  
set Ethernet channel 0 IPv4 configuration method 172  
set Ethernet channel 0 MTU 174  
set Ethernet channel 0 static IP address (IPv4) 166  
set Ethernet channel 0 static IP address (IPv6) 167  
set Ethernet channel 0 subnet mask (IPv4) 171  
set first LDAP server host name 206  
set first LDAP server IP address 206  
set first LDAP server port number 207  
set fourth LDAP server host name 207  
set fourth LDAP server IP address 207  
set fourth LDAP server port number 208  
set FTP data port number 243  
set FTP port number 242  
set FTP timeout 251  
set global VLAN state 372  
set HTTP port number 243  
set HTTPS port number 243  
set IP address (IPv4) 166, 168  
set IP address (IPv6) 167–168  
set LDAP client distinguished name 210  
set LDAP client distinguished name password 210  
set LDAP client distinguished name password (confirm) 210  
set LDAP group filter 203  
set LDAP group search attribute 203  
set LDAP login permission attribute 204  
set LDAP name 204  
set LDAP root distinguished name 208  
set LDAP security version 202  
set LDAP server binding method 209  
set LDAP server discovery method 205  
set LDAP server domain name 205  
set LDAP server for authentication only 209  
set LDAP server forest name 205  
set LDAP UID search attribute 209  
set location 99  
set logical link loss alert and failover policy 352  
set maximum LDAP sessions for user 42  
set maximum number of login failures 41  
set maximum number of simultaneous sessions for  
  user 360  
set minimum number of different characters for  
  password 40  
set name 96  
set NTP server hostname 225  
set NTP server IP address 225  
set NTP server key 227

set NTP update frequency 226  
 set password expiration time 43  
 set password minimum change interval 43  
 set password reuse cycle 44  
 set second LDAP server host name 206  
 set second LDAP server IP address 206  
 set second LDAP server port number 207  
 set secure TCP command mode port number 246  
 set security policy (chassis) 289  
 set serial port baud rate 238  
 set serial port communication rate 238  
 set serial port parity 239  
 set serial port stop bits 239  
 set server host name 294  
 set server IP address 294  
 set SLP port number 244  
 set SMTP e-mail server domain name 294  
 set SNMP agent port number 244  
 set SNMP community 1 first host name 297  
 set SNMP community 1 first host name - get 299  
 set SNMP community 1 first host name to set 298  
 set SNMP community 1 IP address (first host) 297  
 set SNMP community 1 IP address (first host) to get 299  
 set SNMP community 1 IP address (first host) to set 298  
 set SNMP community 1 IP address (second host) 299  
 set SNMP community 1 IP address (third host) 300  
 set SNMP community 1 name 297  
 set SNMP community 1 second host name 299  
 set SNMP community 1 third host name 300  
 set SNMP community 1 view type (SNMPv3) 300  
 set SNMP community 2 first host name 301  
 set SNMP community 2 IP address (first host) 301  
 set SNMP community 2 IP address (second host) 302  
 set SNMP community 2 IP address (third host) 303  
 set SNMP community 2 name 301  
 set SNMP community 2 second host name 302  
 set SNMP community 2 third host name 303  
 set SNMP community 2 view type (SNMPv3) 303  
 set SNMP community 3 first host name 304  
 set SNMP community 3 IP address (first host) 304  
 set SNMP community 3 IP address (second host) 305  
 set SNMP community 3 IP address (third host) 306  
 set SNMP community 3 name 304  
 set SNMP community 3 second host name 305  
 set SNMP community 3 third host name 306  
 set SNMP community 3 view type (SNMPv3) 306  
 set SNMP contact name 307  
 set SNMP location 307  
 set SNMP traps port number 245  
 set SSH port number 246  
 set syslog event log collector 1 IP address 330  
 set syslog event log collector 1 port number 331  
 set syslog event log collector 2 IP address 331  
 set syslog event log collector 2 port number 332  
 set syslog filter level 329  
 set TCP command mode port number 245  
 set TCP command-mode timeout 251  
 set Telnet port number 246  
 set Telnet port timeout 252  
 set TFTP port number 247  
 set third LDAP server host name 206  
 set third LDAP server IP address 206  
 set third LDAP server port number 208  
 set time 107  
 set time zone 107  
 set trespass feature message 338  
 set trespass feature to default 338  
 set tsyslog event log collector 1 host name 330  
 set tsyslog event log collector 2 host name 331  
 set user authentication method 39  
 set user permission groups 359  
 set web interface inactivity timeout 44  
 smtp commands 293, 295  
 SMTP settings commands  
   example 295  
 snmp commands 295, 308  
 SNMP settings commands  
   example 308  
 SSH connection 21  
 sshcfg command 315–316  
   example 316  
 SSL certificate status 317  
 SSL status 317  
 synchronize with NTP server 227  
 terminate user session 355  
 trespass command 337, 339  
   example 339  
 turn secure TCP command mode on or off 250, 342  
 turn TCP command mode on or off 250, 341  
 unacknowledge call-home activity log entry 78  
 unlock user 356  
 update SSH public key 364  
 uplink configuration 350  
 upload (add) SSH public key 362  
 upload (update) SSH public key 362  
 view configuration 214  
 view power management policy 236  
 virtual reset 291  
 virtual reset (suppress warnings) 292  
 write command 383–384  
   example 384  
 CMM (primary with override)  
   reset 277  
 CMM (primary)  
   command target 125  
   display Ethernet channel 0 configuration 165  
   display Ethernet channel 0 DHCP configuration 109  
   reset 277  
   set Ethernet channel 0 domain name 175  
   set Ethernet channel 0 MAC address 174  
 CMM (standby)  
   command target 125  
   display Ethernet channel 0 configuration 165  
   display Ethernet channel 0 DHCP configuration 109  
   reset 278  
   set Ethernet channel 0 domain name 176  
   set Ethernet channel 0 hostname 172  
   set Ethernet channel 0 MAC address 175  
   set Ethernet channel 0 static IP address (IPv4) 169  
   set Ethernet channel 0 static IP address (IPv6) 169  
   set IP address (IPv4) 169  
   set IP address (IPv6) 169  
 CMM air filter command 47  
 CMM CA  
   view self-signed certificate 318  
 CMM connection information 17  
 CMM failover commands 349  
 CMM firmware 1  
 CMM fsmcm command 137  
 CMM HTTPS server  
   generate CSR 319  
 CMM redundancy failure 45, 349  
 CMM uplink failover commands  
   example 353  
 CMM VLAN settings  
   commit 371  
 CMM, group LDAP authentication 150  
 CMM, user accounts 353  
 CMM, user permission group 228  
 collect service data  
   compute node 285  
 command  
   health 156, 159  
   system physical configuration 214  
 command authority 10  
 command environment selecting 6  
 command help 161  
 command history 163  
 command redirect 35, 124  
 command syntax 35

- command target 35, 124
  - add-in card 126
  - alarm panel 126
  - BMC 126
  - CMM 125
  - CMM (primary) 125
  - CMM (standby) 125
  - compute node 125–126
  - compute node (in logical node grouping) 126
  - DIMM, flash 126
  - expansion adapter 126
  - expansion node 126
  - fan logic module 128
  - fan module 128
  - flash DIMM 126
  - Flex System Enterprise Chassis 125
  - high-speed expansion card 126
  - integrated system-management processor 126
  - I/O module 127
  - logical node grouping 125
  - management card 126
  - management processor 126
  - memory 126
  - microprocessor 126
  - node system-management processor 126
  - power supply 128
  - rear LED card 128
  - storage backplane 126
  - storage expansion enclosure 128
  - switch module 127
  - system-management processor 126
  - temporary 7
  - view 214
- command target selection 6
- command targeting
  - example 8
- command-line interface
  - disable for CMM 340
  - enable for CMM 340
  - errors 385
  - guidelines 5
    - case sensitivity 5
    - command history 6
    - data types 6
    - delimiters 6
    - help 6
    - options 5
    - output format 6
    - strings 6
  - introduction 1
  - starting 16
  - using 5, 35
- commands
  - accseccfg 35, 44
  - Active Directory, group authentication 150
  - advfailover 45, 47
  - airfilter 47
  - alertcfg 48–49
  - alertentries 50, 56
  - autoftp 57, 59
  - baydata 59, 64
  - bootmode 64–65
  - bootseq 66–67
  - chconfig 69, 75
  - chlog 76, 78
  - chmanual 79–80
  - cimsub 82
  - cimsub command 81
  - cin 89
  - cin command 84
  - cinstatus 90
  - cinstatus command 90
  - clear 91, 93
  - clear CMM event log 93–94
  - clearlog 93–94
  - clock 106, 108
  - CMM failover 349, 353
  - config 95, 99
  - console 100–101
  - coolingzones 101–102
  - crypto 103, 105
  - date 106
  - dhcpinfo 108, 111
  - display CMM call-home events in events log 76
  - display CMM event log 112, 117
  - displaylog 112, 117
  - displaysd 118
  - dns 120, 123
  - environment 124, 128
  - ethoverusb 129–130
  - event log, clear for CMM 93–94
  - event log, display for CMM 76, 112, 117
  - events 131–132
  - examples
    - account security 44
    - accsecfg 44
    - advfailover 47
    - alarm 213
    - alertcfg 49
    - alertentries 56
    - autoftp 59
    - baydata 64
    - bootmode 65
    - bootseq 67
    - chconfig 75
    - chlog 78
    - chmanual 80
    - cimsub 82
    - cin 89
    - cinstatus 90
    - clear 93
    - clear CMM event log 94
    - clearlog 94
    - clock 108
    - CMM DNS 123
    - CMM Ethernet network settings 191
    - CMM event log clear 94
    - CMM event log display 117
    - CMM LDAP configuration 210
    - CMM name 99
    - CMM network port configuration 253
    - CMM restore configuration 273
    - CMM save configuration 384
    - CMM serial port settings 239
    - CMM SMTP settings 295
    - CMM SNMP settings 308
    - CMM SSH 316
    - CMM uplink failover 353
    - compute node name 99
    - config 99
    - configure automated message settings 59
    - console 101
    - coolingzones 102
    - crypto 105
    - dhcpinfo 111
    - display automated message settings 59
    - display call-home owner 80
    - display CMM chassis security 289
    - display CMM event log 117
    - display CMM security (chassis) 289
    - display Service Advisor owner 75
    - display service information owner 287
    - displaylog 117
    - displaysd 118
    - DNS 123
    - env 128
    - environment 128
    - environment redirect 129
    - Ethernet network settings for CMM 191
    - ethoverusb 130

- events 132
- exit 134
- files 134
- fod 136
- fruactlog 136
- fuelg 148
- groups 155
- health 159
- help 161
- history 163
- ifconfig 191
- info 196
- iocomp 200
- LDAP configuration for CMM 210
- ldapcfg 210
- list 214
- monalerts 224
- name for CMM 99
- name for compute node 99
- network port configuration for CMM 253
- ntp 227
- permggroups 232
- ping 234
- pmpolicy 236
- portcfg 239
- ports 253
- power 260
- pwrprofile 268
- read 273
- remotechassis 275
- reset 279
- restore configuration for CMM 273
- save configuration for CMM 384
- scale 281
- sddump 286
- sdemail 287
- security 289
- Serial Over LAN 314
- serial port settings for CMM 239
- service 293
- set call-home 80
- set CMM chassis security 289
- set CMM security (chassis) 289
- set Service Advisor 75
- set service information 287
- smtp 295
- SMTP settings for CMM 295
- snmp 308
- SNMP settings for CMM 308
- sol 314
- SSH configuration for CMM 316
- sshcfg 316
- sslcfg 327
- syntax help 161
- syslog 333
- tcpcmdmode 336
- temps 336
- trespass 339
- uicfg 342
- update 349
- uplink 353
- user account security 44
- user interface configuration 342
- users 367
- vlan 381
- volts 383
- write 384
- exit 133–134
- files 134
- fod 135–136
- fruactlog 136
- fsmcm 137
- fuelg 139, 148
- group authentication, Active Directory 150
- groups 150, 155
- help 160–161
- history 163
- ifconfig 164, 191
- info 192, 196
- iocomp 199–200
- ldapcfg 201, 210
- led 211, 213
- list 214
- monalerts 215, 224
- ntp 224, 227
- permggroups 228, 232
- ping 232, 234
- pmpolicy 235–236
- portcfg 237, 239
- ports 240, 253
- power 254, 260
- power management policy 235
- pwrprofile 260, 268
- read 269, 273
- remotechassis 273, 275
- reset 277, 279
- scale 279, 281
- sddump 284, 286
- sdemail 286–287
- security 287, 289
- Serial Over LAN 308, 314
- service 290, 293
- smtp 293, 295
- snmp 295, 308
- SOL 308, 314
- sshcfg 315–316
- sslcfg 317, 327
- syslog 328, 333
- tcpcmdmode 333, 336
- temps 336
- trespass 337, 339
- uicfg 339, 342
- update 343, 349
- uplink 349, 353
- user interface configuration 339, 342
- users 353, 367
- vlan 371, 381
- volts 382–383
- write 383–384
- commit
  - CMM VLAN settings 371
- commit timeout
  - CMM VLAN settings 372
- common errors 385
- common information model
  - disable for CMM 340
  - enable for CMM 340
- common information model subscription 81
- communicating with Flex System Manager software 333
- communication
  - out-of-band 333
  - test compute node IP address 234
  - test I/O-module IP address 234
  - test IP address (compute node) 233–234
  - test IP address (I/O module) 233
  - test IP address (I/O-module) 234
- communication rate
  - set for serial port of CMM 238
- compatibility
  - I/O module
    - display details for compute node 200
    - display details for I/O module 200
    - display for all components 200
- component and reloading information 192
- component information display 193
- compute node 178
  - bay data 60
  - collect service data 285
  - command target 125–126
  - config command 95, 99

- example 99
- cycle power 256
- dhcpinfo commands 108
- disable DHCPv6 184
- disable IPv4 182
- disable IPv6 stateless auto-configuration 184
- disable SMS 255
- display bay data 60
- display boot mode 65
- display boot sequence 66
- display Ethernet-over-USB setting 130
- display IP addresses 233
- display name 95
- display network configuration status 177
- display power state 257
- display temperature 336
- display voltage 383
- dump service data 285
- enable centralized user account management (IPMI/  
SNMPv3) 366
- enable DHCPv6 configuration 184
- enable dynamic power optimizer 147
- enable dynamic power optimizer, extended 147
- enable IPv4 182
- enable IPv6 stateless auto-configuration 184
- enable local power control 258
- enable power capping 146
- enable power management 146
- enable power saver mode 146
- enable SMS 255
- enable Wake on LAN 257
- get service data 285
- power off 256
- power on 255–256
- power on (to console) 255–256
- reset 277
- reset (to console) 278
- reset (with NMI) 279
- service commands 290
- set address prefix length 183
- set automatic power-on policy 258
- set boot mode 65
- set boot sequence 66
- set Ethernet-over-USB setting 130
- set IP address (IPv4) 178
- set IP address (IPv6) 178
- set name 97
- set network interface gateway IP address (IPv4) 179
- set network interface gateway/default route (IPv6) 180
- set network interface IPv4 configuration method 181
- set network interface subnet mask (IPv4) 181
- set power capping 145
- set restart delay 259
- shutdown 256
- turn off 256
- turn on 255–256
- turn on (to console) 255–256
- virtual reseal 291
- compute node (all interfaces)
  - display management network DHCP configuration 110
- compute node (in logical node grouping)
  - command target 126
- compute node (specific interface)
  - display management network DHCP configuration 111
- compute node IP address
  - ping 234
  - test communication 234
- compute node management processor
  - hard restart 293
  - hardware reset 293
- compute node power information display (overview) 139
- compute node system-management processor
  - hard restart 293
  - hardware reset 293
- compute node, display power trending 142
- compute nodes
  - disable centralized user account management (IPMI/  
SNMPv3) 366
- config 95
  - options
    - contact 99
    - loc 99
    - name 96–97
    - rack 97
    - rackunit 98
    - room 98
- config command 95
  - example 99
- config command errors 399
- configuration
  - backup 383
  - restore 269
  - save for CMM (to file) 384
  - view for CMM 214
  - view tree for system 214
- configuration changes (IPv4)
  - apply for CMM 167
- configuration from file
  - restore (verbose) CMM 271
  - restore (verbose) CMM and reset 273
  - restoreCMM 271
  - restoreCMM and reset 272
- configuration information
  - display for network interface 177
- configuration method (IPv4)
  - set for channel 0 of CMM 172
  - set for network interface of compute node 181
- configure LDAP command
  - example 210
- configure network ports command
  - example 253
- confirm password
  - LDAP distinguished name 210
- connection information
  - CMM 17
- console 101
  - create override SOL session 101
  - create SOL session 101
  - non-persistent session 101
  - options
    - l 101
    - o 101
  - persistent console 101
- console command 100
- console command errors 400
- console commands
  - example 101
- contact information
  - Service Advisor 71
  - Service Advisor (alternate) 73
- contact information, Service Advisor
  - city 71
  - company 71
  - contact name 71
  - country 71
  - email address 71
  - machine location phone number 71
  - phone extension 71
  - phone number 71
  - postal code 71
  - state 71
  - street address 71
- contact information, Service Advisor (alternate)
  - city 73
  - contact name 73
  - country 73
  - email address 73
  - machine location phone number 73
  - phone extension 73
  - phone number 73

- postal code 73
- state 73
- street address 73
- contact name
  - display for CMM 95
  - set for CMM 99
- contamination, particulate and gaseous 467
- cooling zone health
  - display 101
- cooling zone information
  - display for all 102
  - display for specific zone 102
- coolingzones 102
- coolingzones command errors 401
- coolingzones commands 101
  - example 102
- create
  - VLAN entry 374
- create alert recipient 51
- create CIN configuration entry 87
- create CIN index entry 87
- create override SOL session 101
- create SOL session 101
  - persistent console 101
- create user 357
- creating a personalized support web page 462
- critical alerts
  - disable monitoring for all 216
  - disable monitoring for chassis 217
  - disable monitoring for cooling device 217
  - disable monitoring for I/O module 217
  - disable monitoring for node device 216
  - disable monitoring for power supply 218
  - disable monitoring for system management 217
  - enable monitoring for all 216
  - enable monitoring for chassis 217
  - enable monitoring for cooling device 217
  - enable monitoring for I/O module 217
  - enable monitoring for node device 216
  - enable monitoring for power supply 218
  - enable monitoring for system management 217
- crypto 104
  - options
    - cs 104
    - m 104
- crypto command 103
  - example 105
- crypto command errors 402
- cryptographic mode
  - set for CMM 104
- cryptographic settings
  - display for CMM 104
  - set for CMM 104
- CSR
  - generate for CMM HTTPS server 319
  - generate for LDAP client 319
- CSR (SSL)
  - download certificate file (format) 322
- CSR authentication
  - using CLI 28
  - using web interface 28
- CSR import (mutual authentication)
  - using CLI 31
- custom support web page 462
- cycle power
  - compute node 256
  - I/O module 256
  - switch module 256

## D

- Danger notice, meaning 2
- data rate

- set for channel 0 of CMM 173
- date 106
  - display for CMM 106
  - options
    - d 107
    - t 107
    - tz 106–107
    - tz, v 106
  - set for CMM 107
- date command errors 403
- date commands 106
- daylight-savings time setting
  - display for CMM 106
- default configuration
  - restore for CMM 91
- default IP address 17
- delete
  - VLAN entry (all) 373
  - VLAN entry (specific) 374
- delete Active Directory group 155
- delete alert recipient 51
- delete CIN configuration 86
- delete file
  - CMM 134
- delete power group 267
- delete power schedule 268
- delete user 356
- delete user permission group 231
- destination
  - display for CIM subscriptions 82
- DHCP configuration
  - display for I/O module 111
- dhcpinfo 110–111
  - options
    - eth0 109
    - eth0, standby 109
    - interface 111
- dhcpinfo command errors 404
- dhcpinfo commands 108
  - example 111
- DHCPv6
  - disable for CMM 177
  - disable for compute node 184
  - disable for I/O module 191
  - enable for CMM 177
  - enable for compute node 184
  - enable for I/O module 191
- DIMM, flash
  - command target 126
- disable
  - centralized account management 137
  - centralized user account management 138
  - CLI SFTP server for CMM 316
  - CLI SSH server for CMM 316
  - enhanced legacy alert categories 216
  - global VLAN state 372
  - LDAP (secure) 317
  - logging of login events from same IP address 41
  - monitoring for all critical alerts 216
  - monitoring for all informational alerts 220
  - monitoring for all warning alerts 218
  - monitoring for chassis critical alerts 217
  - monitoring for chassis informational alerts 221
  - monitoring for chassis warning alerts 219
  - monitoring for cooling device critical alerts 217
  - monitoring for cooling device informational alerts 224
  - monitoring for cooling device warning alerts 220
  - monitoring for event log informational alerts 222
  - monitoring for event log warning alerts 219
  - monitoring for inventory change informational alerts 222
  - monitoring for I/O module critical alerts 217
  - monitoring for I/O module informational alerts 221
  - monitoring for I/O module warning alerts 219
  - monitoring for network change informational alerts 223
  - monitoring for node device critical alerts 216

- monitoring for node device informational alerts 221
- monitoring for node device warning alerts 218
- monitoring for power state informational alerts 222
- monitoring for power supply critical alerts 218
- monitoring for power supply informational alerts 224
- monitoring for power supply warning alerts 220
- monitoring for system management critical alerts 217
- monitoring for system management informational alerts 221
- monitoring for system management warning alerts 219
- monitoring for user activity informational alerts 223
- non-fixed VLAN state 373
- secure LDAP 317
- secure TCP command mode 335
- Service Advisor 71
- sol access (VLAN) 375
- SSL for HTTPS server 318
- SSL for LDAP client 317
- syslog event log transmission for collector 1 329
- syslog event log transmission for collector 2 330
- TCP command mode 334
- user account management (centralized) 138
- VLAN sol access 375
- VLAN tagging 376
- disable CIM
  - CMM 248, 340
- disable CIN configuration entry 87
- disable CMM centralized user account management (IPMI/SNMPv3) 367
- disable command-line interface
  - CMM 340
- disable compute nodes centralized user account management (IPMI/SNMPv3) 366
- disable DHCPv6
  - CMM 177
  - compute node 184
  - I/O module 191
- disable DNS
  - CMM 121
- disable Ethernet interface
  - I/O module 189
- disable external management
  - I/O module 189
- disable external ports
  - I/O module 189
- disable FTP
  - CMM 247
- disable HTTPS port
  - CMM 248
- disable IPv4
  - compute node 182
- disable IPv6 stateless auto-configuration
  - CMM 177
  - compute node 184
  - I/O module 191
- disable logical uplink failover
  - CMM 351
- disable network interface
  - CMM (standby) 46
- disable NTP
  - CMM 248
- disable port
  - switch 253
- disable power domain acoustic mode 144
- disable protected mode
  - I/O module 190
- disable secure TCP command mode
  - CMM 250, 342
- disable SFTP
  - CMM 247
- disable SLP
  - CMM 248
- disable SMS
  - compute node 255
- disable SNMP traps
  - CMM 249
- disable SNMPv1
  - CMM 341
- disable SNMPv1 agent
  - CMM 249
- disable SNMPv3
  - CMM 341
- disable SNMPv3 agent
  - CMM 249
- disable SOL
  - global 312
- disable SSH port
  - CMM 249
- disable static IPv6 configuration
  - CMM 176
  - I/O module 190
- disable TCP command mode
  - CMM 250, 341
- disable Telnet port
  - CMM 250
- disable TFTP
  - CMM 251
- disable user 355
- disable web interface
  - CMM 342
- discovered Flex System Enterprise Chassis
  - clear list 275
  - display all 274
  - display filtered by IP address 274
  - display filtered by name 275
  - display health for all 274
- display
  - alert state 216
  - chassis module activity 136
  - clock settings, CMM 106
  - current power management policy 236
  - date, CMM 106
  - daylight-savings time setting, CMM 106
  - GMT offset, CMM 106
  - management channel path information (compute node) 195
  - management channel path information (I/O module) 195
  - power management policy 236
  - TCP command-mode session status 334
  - TCP command-mode session timeout 334
  - time, CMM 106
  - timezone settings 106
  - timezone settings (verbose) 106
  - VLAN settings (all) 371
  - VLAN settings (for ID) 371
- display (reset counter) event log
  - CMM 113
- display active users 354
- display activity
  - chassis module 136
- display advanced failover settings
  - CMM 46
- display air flow trending (chassis) 143
- display alert properties (all recipients) 50
- display alert properties (single recipient) 50
- display alerts 158
  - timestamp 159
- display all Active Directory groups 151
- display all event log entries
  - CMM 113
- display all event log filters
  - CMM 114
- display all Flex System Enterprise Chassis on network 274
- display all information
  - scalable complex 280
- display all power groups 261
- display all power schedules 261
- display all user permission groups 228
- display all users 354
- display boot mode
  - compute node 65
- display call-home activity log



- CMM 77
- display call-home event CMM event log entries 76
- display chassis fault LED states
  - LED states 212
- display chassis LED states
  - LED states 212
- display CIN configuration table 85
- display CMM account security settings 36
- display CMM chassis security policy 289
- display CMM event log commands 112
  - example 117
- display CMM security policy (chassis) 289
- display CMM status 118
- display complete SSH public key 363
- display component information 193
- display compute node power information overview 139
- display configuration information
  - network interface 177
- display contact name
  - CMM 95
- display cooling zone health 101
- display cooling zone information (all) 102
- display cooling zone information (specific) 102
- display cryptographic settings
  - CMM 104
- display destination
  - CIM subscriptions 82
- display DHCP configuration
  - I/O module 111
- display DNS configuration
  - CMM 120
- display DSA host key information
  - CMM 315
- display entries of CIN status table 90
- display Ethernet channel 0 configuration
  - CMM (primary) 165
  - CMM (standby) 165
- display Ethernet channel 0 DHCP configuration
  - CMM (primary) 109
  - CMM (standby) 109
- display Ethernet-over-USB setting
  - compute node 130
- display event log
  - CMM 113
- display event log entries filtered by date
  - CMM 114
- display event log entries filtered by severity level
  - CMM 115
- display event log entries filtered by source
  - CMM 115–116
- display events list
  - CMM 132
- display exhaustive heat trending information (chassis) 142
- display failover configuration
  - CMM 350
- display fan module health 101
- display fan module information 102
- display fan module power information 140
- display fan module temperature 140
- display features
  - CMM 135
  - I/O module 135
- display file list
  - CMM 134
- display firmware attributes 344
- display free space
  - CMM 132, 134
- display FTP/TFTP server call-home activity log
  - CMM 77
- display global remote alert settings
  - CMM 48
- display health for each Flex System Enterprise Chassis on network 274
- display health status 157–158
  - timestamp 159
- display health status (tree) 157
- display information for boot device 66
- display I/O module compatibility
  - all components 200
- display I/O module compatibility details
  - compute node 200
  - I/O module 200
- display I/O module power information 140
- display IP addresses
  - compute node 233
  - I/O module 233
- display LDAP settings
  - CMM 202
- display LED state
  - fan logic module 212
  - fan module 212
  - fan module fault 212
  - fanpack 212
  - for compute node front panel 212
  - for rear LED card 212
- display Lenovo Support call-home activity log
  - CMM 78
- display licenses
  - CMM 135
  - I/O module 135
- display location
  - CMM 95
- display log entries with auxiliary data
  - CMM 114
- display log entries with call-home events
  - CMM 113
- display log entries with Event ID
  - CMM 113
- display log entries with log sequence number
  - CMM 113
- display management network DHCP configuration
  - compute node (all interfaces) 110
  - compute node (specific interface) 111
- display name
  - CMM 95
  - compute node 95
  - Flex System Enterprise Chassis 95
- display network configuration status
  - compute node 177
- display network port settings
  - CMM 241
  - switch 252
- display network settings
  - I/O module 185
- display node information
  - scalable complex 281
- display NTP configuration
  - CMM 225
  - I/O module 225
- display open ports
  - CMM 241
- display partition information
  - scalable complex 281
- display POST status
  - I/O module 259
  - switch module 259
- display power domain information details 140
- display power domain information overview 139
- display power group 261
- display power state
  - compute node 257
  - I/O module 257
  - switch module 257
- display power trending (compute node) 142
- display power trending (fan module) 142
- display power trending (I/O module) 142
- display power trending (power domain) 141
- display power trending (rear LED card) 142
- display power trending (system) 142
- display rack

Flex System Enterprise Chassis 95  
 display rack unit  
   Flex System Enterprise Chassis 95  
 display rear LED card temperature 140  
 display room  
   Flex System Enterprise Chassis 95  
 display RSA host key information  
   CMM 315  
 display serial port configuration  
   CMM 238  
 display Service Advisor 70  
 display service data command 118  
 display SFTP status  
   CMM 315  
 display single user 355  
 display SMTP server host name  
   CMM 294  
 display SMTP server IP address  
   CMM 294  
 display SNMP configuration  
   CMM 296  
 display specific Active Directory groups 151  
 display specific complex information  
   scalable complex 280  
 display specific user permission group 228  
 display SSH public key 363  
 display SSH status  
   CMM 315  
 display state of -lse option  
   CMM 116  
 display status  
   CIM subscriptions 82  
 Display status of first five CIN entries 90  
 display syslog configuration  
   CMM 329  
 display temperature  
   CMM 336  
   compute node 336  
   rear LED card 336  
 display trespass feature status  
   CMM 337  
 display uplink configuration  
   CMM 350  
 display user interface settings  
   CMM 340  
 display voltage  
   compute node 383  
 displaylog 113  
   display log entries with call-home events 113  
   display log entries with Event ID 113  
   display state of -lse option 116  
   filter log entries by call-home events flag 116  
   options  
     -lse 116  
     a 113  
     aux 114  
     c 113  
     ch 116  
     date 114  
     e 113  
     f 113  
     filters 114  
     lse 117  
     sev 115  
     sn 113  
     src 115–116  
     u 117  
 displaylog command errors 404  
 displaylog commands 112  
   example 117  
 displaysd  
   options  
     mmstat 118  
     u 118  
     u, o 118  
 displaysd command errors 406  
 displaysd commands 118  
   example 118  
 distinguished name  
   LDAP client 210  
 distinguished name password  
   LDAP client 210  
 distinguished name password (confirm)  
   LDAP client 210  
 dns 120  
   options  
     -ddns 121  
     i1 121  
     i2 122  
     i3 122  
     i61 122  
     i62 123  
     i63 123  
     on 120–121  
     p 123  
 DNS  
   disable for CMM 121  
   enable for CMM 120  
 dns command errors 408  
 dns commands 120  
   example 123  
 DNS configuration  
   display for CMM 120  
 DNS first IPv4 IP address  
   set for CMM 121  
 DNS first IPv6 IP address  
   set for CMM 122  
 DNS second IPv4 IP address  
   set for CMM 122  
 DNS second IPv6 IP address  
   set for CMM 123  
 DNS server priority  
   set for CMM 123  
 DNS third IPv4 IP address  
   set for CMM 122  
 DNS third IPv6 IP address  
   set for CMM 123  
 documentation  
   using 462  
 Domain Catalog discovery  
   set search domain 205  
 domain name  
   set for channel 0 of CMM (primary) 175  
   set for channel 0 of CMM (standby) 176  
   set for CMM LDAP server 205  
 download  
   LDAP trusted certificate 1 324  
   LDAP trusted certificate 2 325  
   LDAP trusted certificate 3 325  
 download certificate file  
   CA self-signed root certificate 321  
 download certificate file (format)  
   SSL certificate 322  
   SSL CSR 322  
 download SSH public key 363  
 DSA host key information  
   display for CMM 315  
 DSA, sending data 462  
 dump service data  
   compute node 285  
   I/O module 285  
 duplex mode  
   set for channel 0 of CMM 173  
 dynamic DNS  
   enable for CMM 121  
 dynamic power optimizer, enable for compute node 147  
 dynamic power optimizer, extended , enable for compute node 147

## E

- electronic emission Class A notice 468
- email alerts
  - exclude service information 49
  - include service information 49
- enable
  - CLI SFTP server for CMM 316
  - CLI SSH server for CMM 316
  - enhanced legacy alert categories 216
  - global VLAN state 372
  - LDAP (secure) 317
  - monitoring for all critical alerts 216
  - monitoring for all informational alerts 220
  - monitoring for all warning alerts 218
  - monitoring for chassis critical alerts 217
  - monitoring for chassis informational alerts 221
  - monitoring for chassis warning alerts 219
  - monitoring for cooling device critical alerts 217
  - monitoring for cooling device informational alerts 224
  - monitoring for cooling device warning alerts 220
  - monitoring for event log informational alerts 222
  - monitoring for event log warning alerts 219
  - monitoring for inventory change informational alerts 222
  - monitoring for I/O module critical alerts 217
  - monitoring for I/O module informational alerts 221
  - monitoring for I/O module warning alerts 219
  - monitoring for logging of login events from same IP address 41
  - monitoring for network change informational alerts 223
  - monitoring for node device critical alerts 216
  - monitoring for node device informational alerts 221
  - monitoring for node device warning alerts 218
  - monitoring for power state informational alerts 222
  - monitoring for power supply critical alerts 218
  - monitoring for power supply informational alerts 224
  - monitoring for power supply warning alerts 220
  - monitoring for system management critical alerts 217
  - monitoring for system management informational alerts 221
  - monitoring for system management warning alerts 219
  - monitoring for user activity informational alerts 223
  - non-fixed VLAN state 373
  - secure LDAP 317
  - secure TCP command mode 335
  - Service Advisor 71
  - sol access (VLAN) 375
  - SSL for HTTPS server 318
  - SSL for LDAP client 317
  - syslog event log transmission for collector 1 329
  - syslog event log transmission for collector 2 330
  - TCP command mode 335
  - VLAN sol access 375
  - VLAN tagging 376
- enable CIM
  - CMM 248, 340
- enable CIN configuration entry 87
- enable CMM centralized user account management (IPMI/SNMPv3) 367
- enable command-line interface
  - CMM 340
- enable complex password for CMM user authentication 39
- enable compute node centralized user account management (IPMI/SNMPv3) 366
- enable default administration password expiration for CMM 40
- enable DHCPv6
  - CMM 177
  - compute node 184
  - I/O module 191
- enable DNS
  - CMM 120
- enable dynamic DNS
  - CMM 121
- enable dynamic power optimizer for compute node 147
- enable dynamic power optimizer, extended, for compute node 147
- enable Ethernet interface
  - I/O module 189
- enable external management
  - I/O module 189
- enable external ports
  - I/O module 189
- enable FTP
  - CMM 247
- enable HTTPS port
  - CMM 248
- enable IPv4
  - compute node 182
- enable IPv6 stateless auto-configuration
  - CMM 177
  - compute node 184
  - I/O module 191
- enable local power control
  - compute node 258
  - globally 257
- enable logical uplink failover
  - CMM 351
- enable monitoring of event log state
  - CMM 117
- enable network interface and allow IP swap
  - CMM (standby) 46
- enable network interface and prevent IP swap
  - CMM (standby) 46
- enable NTP
  - CMM 225, 248
  - I/O module 225
- enable password change at first login to CMM 42
- enable physical uplink failover
  - CMM 350
- enable port
  - switch 253
- enable power capping for chassis 146
- enable power capping for compute node 146
- enable power domain acoustic mode 144
- enable power management for chassis 146
- enable power management for compute node 146
- enable power saver mode for compute node 146
- enable protected mode
  - I/O module 190
- enable secure TCP command mode
  - CMM 250
- enable SFTP
  - CMM 247
- enable SLP
  - CMM 248
- enable SMS
  - compute node 255
- enable SNMP agent
  - CMM (SNMPv1) 296
  - CMM (SNMPv3) 296
- enable SNMP traps
  - CMM 249, 296
- enable SNMPv1
  - CMM 341
- enable SNMPv1 agent
  - CMM 249
- enable SNMPv3
  - CMM 341
- enable SNMPv3 agent
  - CMM 249
- enable SOL
  - global 311
- enable SSH port
  - CMM 249
- enable static IPv6 configuration
  - CMM 176
  - I/O module 190
- enable TCP command mode
  - CMM 250
- enable Telnet port
  - CMM 250

- enable TFTP
  - CMM 251
- enable trespass feature
  - CMM 337
- enable user 356
- enable V3 authentication for NTP
  - CMM 226
- enable Wake on LAN
  - compute node 257
  - globally 257
- enable web interface
  - CMM 342
- encryption algorithms 17
- end session 133
- ending an SOL session 27, 100
- enhanced legacy alert categories
  - disable 216
  - enable 216
- entries of the CIN status table
  - display for CMM 90
- env 125–126
  - options
    - addin 126
    - be 126
    - blade 125
    - bladeenclosure 128
    - bladegroup 125
    - bladegroup, blade 126
    - cpu 126
    - exp 126
    - fan module 128
    - fanmux 128
    - hsec 126
    - mgmtcrd 126
    - mt 128
    - pciexpress 126
    - power 128
    - sp 126
    - stgbkplane 126
    - switch 127
    - system (CMM) 125
    - tap 126
- env command errors 408
- env commands
  - example 128
- environment
  - add-in card 126
  - alarm panel 126
  - BMC 126
  - CMM 125
  - CMM (primary) 125
  - CMM (standby) 125
  - compute node 125–126
  - compute node (in logical node grouping) 126
  - DIMM, flash 126
  - expansion adapter 126
  - expansion node 126
  - fan logic module 128
  - fan module 128
  - flash DIMM 126
  - Flex System Enterprise Chassis 125
  - high-speed expansion card 126
  - integrated system-management processor 126
  - I/O module 127
  - logical node grouping 125
  - management card 126
  - management processor 126
  - memory 126
  - microprocessor 126
  - node system-management processor 126
  - PCI-Express module 126
  - power supply 128
  - rear LED card 128
  - storage backplane 126
  - storage expansion enclosure 128
  - switch module 127
  - system-management processor 126
- environment commands 124
- example 128
- errors
  - accsecfcg command 387
  - advfailover command 389
  - airfilter command 389
  - alertcfg command 389
  - alertentries command 389
  - autoftpc command 390
  - baydata command 391
  - bootmode command 392, 431
  - bootseq command 392
  - chconfig command 393
  - chlog command 395
  - chmanual command 396
  - cimsub command 396
  - cin command 397
  - cinstatus command 398
  - clear command 398
  - clearlog command 399
  - command-line interface 385
  - common 385
  - config command 399
  - console command 400
  - coolingzones command 401
  - crypto command 402
  - date command 403
  - dhcpcfg command 404
  - displaylog command 404
  - displaysd command 406
  - dns command 408
  - env command 408
  - ethoverusb command 408
  - events command 409
  - exit command 409
  - files command 410
  - fod command 410
  - fruactlog command 411
  - fsmcm command 411
  - fuelg command 411
  - groups command 415
  - health command 416
  - help command 417
  - history command 417
  - ifconfig command 417
  - info command 421
  - iocomp command 422
  - ldapcfg command 422
  - led command 423
  - list command 424
  - monalerts command 424
  - ntp command 424
  - permggroups command 425
  - ping command 426
  - pmpolicy command 427
  - portcfg command 427
  - ports command 427
  - power command 429
  - read command 433
  - remotechassis command 434
  - reset command 435
  - scale command 437
  - sddump command 437
  - sdemail command 438
  - security command 438
  - service command 438
  - smtpc command 439
  - snmp command 440
  - sol command 440
  - sshcfg command 442
  - sslcfg command 442
  - syslog command 444
  - tpcmdmode command 445

- temps command 446
- trespass command 446
- uicfg command 446
- update command 447
- uplink command 451
- users command 452
- vlan command 456
- volts command 459
- write command 459
- Ethernet
  - configuring remote connection 25
- Ethernet channel 0 address prefix length
  - set for CMM 176
- Ethernet channel 0 configuration
  - display for CMM (primary) 165
  - display for CMM (standby) 165
- Ethernet channel 0 data rate
  - set for CMM 173
- Ethernet channel 0 DHCP configuration
  - display for primary CMM 109
  - display for standby CMM 109
- Ethernet channel 0 domain name
  - set for primary CMM 175
  - set for standby CMM 176
- Ethernet channel 0 duplex mode
  - set for CMM 173
- Ethernet channel 0 floating IP address (IPv4)
  - set for CMM 168
- Ethernet channel 0 floating IP address (IPv6)
  - set for CMM 168
- Ethernet channel 0 gateway IP address (IPv4)
  - set for CMM 170
- Ethernet channel 0 gateway/default route (IPv6)
  - set for CMM 170
- Ethernet channel 0 hostname
  - set for CMM 171
  - set for standby CMM 172
- Ethernet channel 0 IPv4 configuration method
  - set for CMM 172
- Ethernet channel 0 MAC address
  - set for primary CMM 174
  - set for standby CMM 175
- Ethernet channel 0 MTU
  - set for CMM 174
- Ethernet channel 0 static IP address (IPv4)
  - set for CMM 166
  - set for standby CMM 169
- Ethernet channel 0 static IP address (IPv6)
  - set for CMM 167
  - set for standby CMM 169
- Ethernet channel 0 subnet mask (IPv4)
  - set for CMM 171
- Ethernet interface
  - disable for I/O module 189
  - enable for I/O module 189
- Ethernet network settings for CMM commands
  - example 191
- Ethernet-over-USB setting
  - display for compute node 130
  - set for compute node 130
- ethoverusb 130
  - options
    - s 130
- ethoverusb command errors 408
- ethoverusb commands 129
  - example 130
- European Union EMC Directive conformance statement 468
- event log
  - clear for CMM 94
  - display (reset counter) for CMM 113
  - display all entries for CMM 113
  - display all filters for CMM 114
  - display entries for CMM, filtered by date 114
  - display entries for CMM, filtered by severity level 115
  - display entries for CMM, filtered by source 115–116
  - display for CMM 113
  - display log entries with auxiliary data CMM 114
  - display log entries with log sequence number CMM 113
  - enable monitoring of state 117
  - save 117
- event log, clear for CMM commands 93
- event log, display for call-home event CMM entries 76
- event log, display for CMM commands 112
- events 132
  - options
    - add 132
    - rm 132
- events command errors 409
- events commands 131
  - example 132
- example
  - command targeting 8
- eXFlash Storage DIMM 7, 126
- exhaustive heat trending information, display (chassis) 142
- exit 133
  - CLI 133
- exit codes (CLI)
  - Secure Shell server 22
- exit command 133
- exit command errors 409
- exit commands
  - example 134
- expansion adapter
  - command target 126
- expansion node
  - command target 126
- export
  - LDAP trusted certificate 1 324
  - LDAP trusted certificate 2 325
  - LDAP trusted certificate 3 325
- export SSH public key 363
- external management
  - disable for I/O module 189
  - enable for I/O module 189
- external ports
  - disable for I/O module 189
  - enable for I/O module 189

## F

- failover configuration
  - display for CMM 350
- fan logic module
  - command target 128
- fan module
  - command target 128
- fan module health
  - display 101
- fan module information
  - display 102
- fan module power information display 140
- fan module temperature display 140
- fan module, display power trending 142
- FCC Class A notice 468
- feature licenses
  - display for CMM 135
  - display for I/O module 135
- files 134
  - options
    - d 134
- files command errors 410
- files commands 134
  - example 134
- filter alert type 54
- filter log entries by call-home events flag
  - CMM 116
- firmware
  - display attributes 344

- update 344–345
  - I/O module 346–348
  - switch 346–348
  - verbose 347
- update (verbose) 346
- firmware requirements 1
- firmware update 343
- flash DIMM
  - command target 126
- flash identify LED 213
- flash storage DIMM 7, 126
- Flex System Enterprise Chassis
  - command target 125
  - configuring for CLI 23
  - display name 95
  - display rack 95
  - display rack unit 95
  - display room 95
- Flex System Enterprise Chassis
  - clear list of discovered 275
  - display all discovered 274
  - display filtered by IP address 274
  - display filtered by name 275
  - display health for all discovered 274
- Flex System Manager software
  - communication 333
- floating IP address (IPv4)
  - set for channel 0 of CMM 168
- floating IP address (IPv6)
  - set for channel 0 of CMM 168
- fod 135
- fod command errors 410
- fod commands 135
  - example 136
- forest name
  - set for CMM LDAP server 205
  - set for Global Catalog discovery 205
- fruactlog 136
- fruactlog command errors 411
- fruactlog commands 136
  - example 136
- fsmcm
  - options
    - off 138
- fsmcm command
  - disable centralized account management 137
- fsmcm command errors 411
- FTP
  - disable for CMM 247
  - enable for CMM 247
- FTP data port number
  - set for CMM 243
- FTP port number
  - set for CMM 242
- FTP timeout
  - set for CMM 251
- fuelg 139–140
  - options
    - aft 143
    - am 144
    - dps 147
    - fpop 147
    - har 143
    - hart 143
    - ht 142
    - pcap 145
    - pm 141
    - pme 146
    - ps 146
    - pt 141–142
    - spl 144
    - tt 142
- fuelg command errors 411
- fuelg commands 139
  - example 148

## G

- gaseous contamination 467
- gateway IP address (IPv4)
  - set for channel 0 of CMM 170
  - set for I/O module 187
  - set for network interface of compute node 179
- gateway IP address (IPv6)
  - set for I/O module 187
- gateway/default route (IPv6)
  - set for channel 0 of CMM 170
  - set for network interface of compute node 180
- generate
  - CSR (CMM HTTPS server) 319
  - CSR (LDAP client) 319
  - self-signed certificate (certificate authority) 319
- generate host key
  - CMM 316
- generate syslog test message
  - CMM 332
- generate test alert 56
- Germany Class A statement 468
- get service data
  - compute node 285
- global
  - enable local power control 257
  - enable Wake on LAN 257
- Global Catalog discovery
  - set forest name 205
- global disable
  - SOL 312
- global enable
  - SOL 311
- GMT offset
  - display for CMM 106
- group filter
  - LDAP 203
- group LDAP authentication, CMM 150
- group search attribute
  - LDAP 203
- groups 151
  - options
    - a 153
    - add 152
    - clear 155
- groups command 150
- groups command errors 415
- groups commands
  - example 155
- guidelines
  - case sensitivity 5
  - command history 6
  - data types 6
  - delimiters 6
  - help 6
  - options 5
  - output format 6
  - overview of 5
  - strings 6

## H

- h 161
- hard restart
  - compute node management processor 293
  - compute node system-management processor 293
- hardware requirements 1
- hardware reset
  - compute node management processor 293
  - compute node system-management processor 293
- hardware service and support telephone numbers 463
- health 157
  - display for all Flex System Enterprise Chassis on network 274

- display status 157
- display status (tree) 157
- display status and alerts 158
- display status and alerts with timestamp 159
- options
  - f 158
  - l 157
  - t 159
- health command 156, 159
  - example 159
- health command errors 416
- help 35, 161
  - command 161
  - from the World Wide Web 462
  - from World Wide Web 462
  - sending diagnostic data 462
  - sources of 461
- help command 160
- help command errors 417
- help commands
  - example 161
- high-speed expansion card
  - command target 126
- history 163
- history command 163
- history command errors 417
- history commands
  - example 163
- host key
  - generate for CMM 316
- host name
  - set for channel 0 of CMM 171
  - set for channel 0 of standby CMM 172
- hot air recirculation detection state, set (chassis) 143
- hot air recirculation threshold, set for chassis 143
- HTTP port number
  - set for CMM 243
- HTTP proxy setup
  - Service Advisor 75
- HTTPS port
  - disable for CMM 248
  - enable for CMM 248
- HTTPS port number
  - set for CMM 243

## I

- identify LED
  - blink 213
  - flash 213
  - light 213
  - turn off 213
- ifconfig 177, 185
  - options
    - c 186
    - dhcp6 191
    - down 189
    - em 189
    - ep 189
    - eth0 165
    - eth0, apply 167
    - eth0, c 172
    - eth0, d 173
    - eth0, dhcp6 177
    - eth0, dn 175
    - eth0, f 168
    - eth0, f6 168
    - eth0, g 170
    - eth0, g6 170
    - eth0, i 166
    - eth0, i6 167
    - eth0, ipv6static 176
    - eth0, l 174

- eth0, m 174
- eth0, n 171
- eth0, o 165
- eth0, o, dn 176
- eth0, o, i 169
- eth0, o, i6 169
- eth0, o, l 175
- eth0, o, n 172
- eth0, p6 176
- eth0, r 173
- eth0, s 171
- eth0, sa6 177
- g 187
- g6 187
- i 186
- i6 187
- interface 177
- ipv6static 190
- network interface, c 181
- network interface, dhcp6 184
- network interface, g 179
- network interface, g6 180
- network interface, i 178
- network interface, i6 178
- network interface, ipv4 182
- network interface, p6 183
- network interface, s 181
- network interface, sa6 184
- p6 190
- pip 188
- pm 190
- s 188
- sa6 191
- up 189
- ifconfig command errors 417
- ifconfig commands 164
  - example 191
- import
  - certificate 327
  - LDAP trusted certificate 1 322
  - LDAP trusted certificate 2 323
  - LDAP trusted certificate 3 324
- import (add) SSH public key 362
- import (mutual authentication) of CA
  - using CLI 31
- import (non-mutual authentication) of CA
  - using CLI 30
- import (update) SSH public key 362
- important notices 466
- info 193
  - options
    - path 195
- info command 192
- info command errors 421
- info commands
  - example 196
- information
  - display for boot device 66
  - display for specific scalable complex 280
- information (all)
  - display for scalable complex 280
- information about components and reloading components 192
- information center 462
- information display, component 193
- information display, compute node power (overview) 139
- information display, fan module power 140
- information display, I/O module power 140
- information display, power domain (detailed) 140
- information display, power domain (overview) 139
- information LED
  - turn off 213
- informational alerts
  - disable monitoring for all 220
  - disable monitoring for chassis 221
  - disable monitoring for cooling device 224

- disable monitoring for event log 222
- disable monitoring for inventory change 222
- disable monitoring for I/O module 221
- disable monitoring for network change 223
- disable monitoring for node device 221
- disable monitoring for power state 222
- disable monitoring for power supply 224
- disable monitoring for system management 221
- disable monitoring for user activity 223
- enable monitoring for all 220
- enable monitoring for chassis 221
- enable monitoring for cooling device 224
- enable monitoring for event log 222
- enable monitoring for inventory change 222
- enable monitoring for I/O module 221
- enable monitoring for network change 223
- enable monitoring for node device 221
- enable monitoring for power state 222
- enable monitoring for power supply 224
- enable monitoring for system management 221
- enable monitoring for user activity 223
- integrated system-management processor
  - command target 126
- I/O module
  - command target 127
  - cycle power 256
  - dhcpinfo commands 108
  - disable DHCPv6 191
  - disable Ethernet interface 189
  - disable external management 189
  - disable external ports 189
  - disable IPv6 stateless auto-configuration 191
  - disable protected mode 190
  - disable static IPv6 configuration 190
  - display DHCP configuration 111
  - display feature licenses 135
  - display IP addresses 233
  - display licenses 135
  - display network settings 185
  - display NTP configuration 225
  - display POST status 259
  - display power state 257
  - dump service data 285
  - enable DHCPv6 configuration 191
  - enable Ethernet interface 189
  - enable external management 189
  - enable external ports 189
  - enable IPv6 stateless auto-configuration 191
  - enable NTP 225
  - enable protected mode 190
  - enable static IPv6 configuration 190
  - keep new IP address configuration after reset 188
  - power off 256
  - power on 255–256
  - reset 277
  - reset (extended diagnostics) 279
  - reset (full diagnostics) 279
  - reset (standard diagnostics) 278
  - reset configuration 93
  - revert to old IP address configuration after reset 188
  - service commands 290
  - set address prefix length 190
  - set gateway IP address (IPv4) 187
  - set gateway IP address (IPv6) 187
  - set IP address (IPv4) 186
  - set IP address (IPv6) 187
  - set IPv4 network configuration method 186
  - set NTP update frequency 226
  - set subnet mask (IPv4) 188
  - turn off 256
  - turn on 256
  - virtual reseal 291
- I/O module compatibility
  - display details for compute node 200
  - display details for I/O module 200
  - display for all components 200
  - I/O module power information display 140
  - I/O module, display power trending 142
  - I/O-module
    - set restart delay 259
  - I/O-module IP address
    - ping 234
    - test communication 234
  - IMM
    - login 26, 308
    - IMM, user accounts 354
  - Important notice, meaning 2
  - iocomp 200
  - iocomp command errors 422
  - iocomp commands 199
    - example 200
  - IP address
    - CIN configuration entry 88
    - CIN index entry 88
    - clear for boot device 67
    - display Flex System Enterprise Chassis on network filtered by 274
    - set for boot device 67
  - IP address (compute node)
    - ping 233–234
    - test communication 233–234
  - IP address (I/O module)
    - ping 233
    - test communication 233
  - IP address (I/O-module)
    - ping 234
    - test communication 234
  - IP address (IPv4)
    - set for CMM 166, 168
    - set for compute node 178
    - set for I/O module 186
    - set for standby CMM 169
  - IP address (IPv6)
    - set for CMM 167–168
    - set for compute node 178
    - set for I/O module 187
    - set for standby CMM 169
  - IP address configuration
    - keep new after reset 188
    - revert to old after reset 188
  - IP address, default 17
  - IP addresses
    - display for compute node 233
    - display for I/O module 233
  - IPMI centralized user account management
    - disable for CMM 367
    - disable for compute nodes 366
    - enable for CMM 367
    - enable for compute nodes 366
  - IPv4
    - disable for compute node 182
    - enable for compute node 182
  - IPv4 configuration changes
    - apply to CMM 167
  - IPv4 configuration method (network)
    - set for I/O module 186
  - IPv6 configuration (static)
    - disable for CMM 176
    - disable for I/O module 190
    - enable for CMM 176
    - enable for I/O module 190
  - IPv6 stateless auto-configuration
    - disable for CMM 177
    - disable for compute node 184
    - disable for I/O module 191
    - enable for CMM 177
    - enable for compute node 184
    - enable for I/O module 191
  - ISMP
    - reset 277



## J

Japan Class A electronic emission statement 469

## K

keep new IP address configuration after reset

I/O module 188

Korea Class A electronic emission statement 470

## L

LDAP (secure)

disable 317

enable 317

LDAP certificate import (non-mutual authentication)

using CLI 30

LDAP client

generate CSR 319

LDAP client distinguished name

set for CMM 210

LDAP client distinguished name password

set for CMM 210

LDAP client distinguished name password (confirm)

set for CMM 210

LDAP group filter

set for CMM 203

LDAP group search attribute

set for CMM 203

LDAP login permission attribute

set for CMM 204

LDAP name

set for CMM 204

LDAP root distinguished name

set for CMM 208

LDAP security version

set for CMM 202

LDAP server (first) host name

set for CMM 206

LDAP server (first) IP address

set for CMM 206

LDAP server (first) port number

set for CMM 207

LDAP server (fourth) host name

set for CMM 207

LDAP server (fourth) IP address

set for CMM 207

LDAP server (fourth) port number

set for CMM 208

LDAP server (second) host name

set for CMM 206

LDAP server (second) IP address

set for CMM 206

LDAP server (second) port number

set for CMM 207

LDAP server (third) host name

set for CMM 206

LDAP server (third) IP address

set for CMM 206

LDAP server (third) port number

set for CMM 208

LDAP server authentication method

set for CMM 209

LDAP server binding method

set for CMM 209

LDAP server discovery method

set for CMM 205

LDAP server domain name

set for CMM 205

LDAP server forest name

set for CMM 205

LDAP settings

display for CMM 202

LDAP trusted certificate 1

download 324

export 324

import 322

remove 326

upload 322

LDAP trusted certificate 2

download 325

export 325

import 323

remove 326

upload 323

LDAP trusted certificate 3

download 325

export 325

import 324

remove 327

upload 324

LDAP UID search attribute

set for CMM 209

ldapcfg 202

options

aom 209

bm 209

cd 210

cp 210

dn 205

fn 205

gf 203

gsa 203

i1 206

i2 206

i3 206

i4 207

lpa 204

p 210

p1 207

p2 207

p3 208

p4 208

rd 208

server 205

t 204

usa 209

v 202

ldapcfg command 201

example 210

ldapcfg command errors 422

led 212

options

info 212

info off 213

l 212

loc 212–213

LED (information)

turn off 213

led command 211

led command errors 423

led commands

example 213

LED state

display (compute node front panel) 212

display (rear LED card) 212

display (state for fan logic module LEDs) 212

display (state for fan module fault LED) 212

display (state for fanpack LEDs) 212

display (state for I/O module) 212

display fault for chassis 212

display for chassis 212

Lenovo eXFlash Storage DIMM 7, 126

licenses

display for CMM 135

display for I/O module 135

light identify LED 213

- link local address 18
- list 214
  - options
    - l 214
- list command
  - example 214
- list command errors 424
- local power control
  - enable for compute node 258
  - enable globally 257
- location
  - display for CMM 95
  - set for CMM 99
- location (rack unit)
  - set for chassis 98
- location (rack)
  - set for chassis 97
- location (room)
  - set for chassis 98
- logging
  - disable for logging of login events from same IP address 41
  - enable for logging of login events from same IP address 41
- logical link loss alert and failover policy
  - set for CMM 352
- logical node grouping
  - command target 125
- login
  - IMM 26, 308
- login permission attribute
  - LDAP 204

## M

- MAC address
  - set for channel 0 of CMM (primary) 174
  - set for channel 0 of standby CMM 175
- manage alert recipients 50
- management card
  - command target 126
- management channel path information (compute node)
  - display 195
- management channel path information (I/O module)
  - display 195
- management network DHCP configuration
  - display for compute node (all interfaces) 110
  - display for compute node (specific interface) 111
- management processor
  - command target 126
  - reset 277
- maximum LDAP sessions for user
  - set for CMM 42
- maximum number of login failures
  - set for CMM 41
- memory
  - command target 126
- microprocessor
  - command target 126
- minimum number of different characters for password
  - set for CMM 40
- modify power group 264
- modify power schedule 266
- modify user permission group 230
- module (chassis)
  - display activity 136
- monalerts 216
  - options
    - ca 216
    - cb 216
    - ccd 217
    - ccsm 217
    - ciom 217
    - cpm 218
    - ec 216

- ia 220
- ib 221
- icd 224
- icsm 221
- iel 222
- iinv 222
- iiom 221
- inc 223
- ipm 224
- ipon 222
- iua 223
- wa 218
- wb 218
- wcd 220
- wcsm 219
- wel 219
- wiom 219
- wpm 220
- monalerts command errors 424
- monalerts commands 215
  - example 224
- monitoring
  - disable for all critical alerts 216
  - disable for all informational alerts 220
  - disable for all warning alerts 218
  - disable for chassis critical alerts 217
  - disable for chassis informational alerts 221
  - disable for chassis warning alerts 219
  - disable for cooling device critical alerts 217
  - disable for cooling device informational alerts 224
  - disable for cooling device warning alerts 220
  - disable for event log informational alerts 222
  - disable for event log warning alerts 219
  - disable for inventory change informational alerts 222
  - disable for I/O module critical alerts 217
  - disable for I/O module informational alerts 221
  - disable for I/O module warning alerts 219
  - disable for network change informational alerts 223
  - disable for node device critical alerts 216
  - disable for node device informational alerts 221
  - disable for node device warning alerts 218
  - disable for power state informational alerts 222
  - disable for power supply critical alerts 218
  - disable for power supply informational alerts 224
  - disable for power supply warning alerts 220
  - disable for system management critical alerts 217
  - disable for system management informational alerts 221
  - disable for system management warning alerts 219
  - disable for user activity informational alerts 223
  - enable for all critical alerts 216
  - enable for all informational alerts 220
  - enable for all warning alerts 218
  - enable for chassis critical alerts 217
  - enable for chassis informational alerts 221
  - enable for chassis warning alerts 219
  - enable for cooling device critical alerts 217
  - enable for cooling device informational alerts 224
  - enable for cooling device warning alerts 220
  - enable for event log informational alerts 222
  - enable for event log warning alerts 219
  - enable for inventory change informational alerts 222
  - enable for I/O module critical alerts 217
  - enable for I/O module informational alerts 221
  - enable for I/O module warning alerts 219
  - enable for network change informational alerts 223
  - enable for node device critical alerts 216
  - enable for node device informational alerts 221
  - enable for node device warning alerts 218
  - enable for power state informational alerts 222
  - enable for power supply critical alerts 218
  - enable for power supply informational alerts 224
  - enable for power supply warning alerts 220
  - enable for system management critical alerts 217
  - enable for system management informational alerts 221
  - enable for system management warning alerts 219

- enable for user activity informational alerts 223
- MTU
  - set for channel 0 of CMM 174
- mutual authentication certificate import
  - using CLI 31
- mutual authentication import of CA
  - using CLI 31
- mutual authentication import of CSR
  - using CLI 31

## N

- name
  - display Flex System Enterprise Chassis on network filtered by 275
  - display for CMM 95
  - display for compute node 95
  - set for chassis 96
  - set for CMM 96
  - set for compute node 97
- name (contact)
  - set for CMM 99
- network access tag 17
- network configuration method (IPv4)
  - set for I/O module 186
- network configuration status
  - display for compute node 177
- network interface
  - disable for standby CMM 46
  - display configuration information 177
  - enable for standby CMM and allow IP swap during failover 46
  - enable for standby CMM and prevent IP swap during failover 46
- network interface gateway IP address (IPv4)
  - set for compute node 179
- network interface gateway/default route (IPv6)
  - set for compute node 180
- network interface IPv4 configuration method
  - set for compute node 181
- network interface static IP address (IPv4)
  - set for compute node 178
- network interface static IP address (IPv6)
  - set for compute node 178
- network interface subnet mask (IPv4)
  - set for compute node 181
- network port settings
  - display for CMM 241
  - display for switch 252
  - reset for CMM 242
- network settings
  - display for I/O module 185
- New Zealand Class A statement 468
- NIST 103
- node information
  - display for scalable complex 281
- node system-management processor
  - command target 126
  - reset 277
- non-mutual authentication certificate import
  - using CLI 30
- non-mutual authentication import of CA
  - using CLI 30
- non-mutual authentication import of LDAP certificate
  - using CLI 30
- notes, important 466
- notices 465
  - electronic emission 468
  - FCC, Class A 468
- notification method, set for alerts 55
- ntp 225
  - options
    - en, enabled 225

- f 226
- i 225
- synch 227
- v3 227
- v3en, enabled 226
- NTP
  - disable for CMM 248
  - enable for CMM 225, 248
  - enable for I/O module 225
- ntp command 224
  - example 227
- ntp command errors 424
- NTP configuration
  - display for CMM 225
  - display for I/O module 225
- NTP server
  - synchronize CMM clock 227
- NTP server hostname
  - set for CMM 225
- NTP server IP address
  - set for CMM 225
- NTP server key
  - set for CMM 227
- NTP update frequency
  - set for CMM 226
  - set for I/O module 226

## O

- ommand
  - re-enter previous 163
- online documentation 1
- open ports
  - display for CMM 241
- options
  - a 90
  - clear 82
  - f 90
  - v 82
- out-of-band communication, Flex System Manager software 333
- override persistent command environment 7

## P

- parity
  - set for serial port of CMM 239
- particulate contamination 467
- partition information
  - display for scalable complex 281
- password
  - change for user (other user) 359
  - change for user (own password) 358
  - LDAP distinguished name 210
- password (confirm)
  - LDAP distinguished name 210
- password expiration time
  - set for CMM 43
- password minimum change interval
  - set for CMM 43
- password policy 35
- password reuse cycle
  - set for CMM 44
- path information
  - display for management channel (compute node) 195
  - display for management channel (I/O module) 195
- People's Republic of China Class A electronic emission statement 470
- permggroups 228
  - options
    - add 229
    - clear 231

- n 228
  - n, a 230
- permggroups command 228
- permggroups command errors 425
- permggroups commands
  - example 232
- permission groups
  - backup 383
  - restore 269
- persistent command environment
  - override 7
- persistent command target 6
- ping
  - compute node IP address 234
  - i 233–234
  - I/O-module IP address 234
  - IP address (compute node) 233–234
  - IP address (I/O module) 233
  - IP address (I/O-module) 234
- ping command errors 426
- ping commands 232
  - example 234
- pmpolicy 236
  - options
    - pd 236
    - pm 236
  - view for CMM 236
- pmpolicy command
  - example 236
- pmpolicy command errors 427
- policy
  - password 35
  - security (chassis) 287
- portcfg
  - options
    - com1 238
    - com1, b 238
    - com1, p 239
    - com1, s 239
- portcfg command errors 427
- portcfg commands 237
  - example 239
- ports 241
  - options
    - cime 248
    - cimp 244
    - ftpdp 243
    - ftpe 247
    - ftpp 242
    - ftpt 251
    - http 243
    - httpse 248
    - https 243
    - ntpe 248
    - open 241
    - reset 242
    - sftpe 247
    - slpe 248
    - slpp 244
    - snmp1ae 249
    - snmp3ae 249
    - snmpap 244
    - snmpte 249
    - snmptp 245
    - sshe 249
    - sshp 246
    - stcme, port mode 250
    - stcmp 246
    - tcme, port mode 250
    - tcmp 245
    - tcmt 251
    - telnete 250
    - telnetp 246
    - telnett 252
    - tftpe 251
    - tftpp 247
    - speed 253
    - switch 252
    - switch, state 253
- ports (open)
  - display for CMM 241
- ports command 240
  - example 253
- ports command errors 427
- POST status
  - display for I/O module 259
  - display for switch module 259
- power
  - options
    - ap 258
    - cycle 256
    - cycle, c 256
    - d 259
    - local 257–258
    - off 256
    - on 255
    - on, c 255
    - sms 255
    - softoff 256
    - state 257
    - state, post 259
    - wol 257
  - power capping, enable for chassis 146
  - power capping, enable for compute node 146
  - power capping, set for compute node 145
  - power command errors 429
  - power commands 254
    - example 260
  - power domain
    - disable acoustic mode 144
    - enable acoustic mode 144
  - power domain information display (detailed) 140
  - power domain information display (overview) 139
  - power domain redundancy loss policy, set 141
  - power domain, display power trending 141
  - power group, add 262
  - power group, delete 267
  - power group, display 261
  - power group, display (all) 261
  - power group, modify 264
  - power management policy
    - display 236
    - display current 236
    - set 236
  - power management, enable for chassis 146
  - power management, enable for compute node 146
  - power off
    - compute node 256
    - I/O module 256
    - switch module 256
  - power on
    - compute node 255–256
    - I/O module 255–256
    - switch module 255–256
  - power on (to console)
    - compute node 255–256
  - power saver mode, enable for compute node 146
  - power schedule, add 263
  - power schedule, assign to power group 263
  - power schedule, delete 268
  - power schedule, display (all) 261
  - power schedule, modify 266
  - power state
    - display for compute node 257
    - display for I/O module 257
    - display for switch module 257
  - power supply
    - command target 128
  - power trending, display (compute node) 142
  - power trending, display (fan module) 142

- power trending, display (I/O module) 142
- power trending, display (power domain) 141
- power trending, display (system) 142
- previous command
  - re-enter 163
- primary CMM 8
- problem description
  - call-home 80
  - email 287
  - service information 287
- product service, Taiwan 463
- protected mode
  - disable for I/O module 190
  - enable for I/O module 190
- pwrprofile 261
  - options
    - a 266
    - add 262–263
    - clear 267
    - clear, i 268
    - d 266
    - f 266
    - key 264
    - n 264
    - s 266
    - servers 264
    - t 266
- pwrprofile commands 260
  - example 268

## R

- rack location
  - set for chassis 97
- rack unit location
  - set for chassis 98
- re-enter previous command 163
- read
  - options
    - p, r, u 272
    - p, r, u, v 273
    - u, p 271
    - v, u, p 271
- read CIN configuration status table entries 90
- read CIN status table entries for CMM 90
- read command 269
  - example 273
- read command errors 433
- rear LED card
  - command target 128
  - display temperature 336
- rear LED card temperature display 140
- rear LED card, display power trending 142
- redirect command 35, 124
- redundancy failure
  - CMM 45, 349
- redundancy loss policy, power domain (set) 141
- remote alert
  - set retry limit 49
- remote alerts
  - set retry interval 48
- remotechassis 274
  - options
    - clear 275
    - health 274
    - ip 274
    - name 275
- remotechassis command 273
  - example 275
- remotechassis command errors 434
- remove
  - LDAP trusted certificate 1 326
  - LDAP trusted certificate 2 326

- LDAP trusted certificate 3 327
- remove SSH user public key 361
- required, firmware 1
- required, hardware 1
- reset
  - virtual 290
- reset 277
  - CMM (primary with override) 277
  - CMM (primary) 277
  - CMM (standby) 278
  - compute node 277
  - I/O module 277
  - ISMP 277
  - management module (primary) 277
  - management processor 277
  - node system-management processor 277
  - options
    - c 278
    - exd 279
    - f 278
    - full 279
    - sft 279
    - standby 278
    - std 278
  - service level 290
  - switch module 277
  - system-management processor 277
  - virtual 290
- reset -o 277
- reset (extended diagnostics)
  - I/O module 279
  - switch module 279
- reset (failover)
  - CMM 278
- reset (full diagnostics)
  - I/O module 279
  - switch module 279
- reset (standard diagnostics)
  - I/O module 278
  - switch module 278
- reset (to console)
  - compute node 278
- reset (with NMI)
  - compute node 279
- reset command errors 435
- reset commands 277
  - example 279
- reset compute node key sequence
  - set for SOL 313
- reset configuration
  - I/O module 93
  - switch module 93
- reset configuration (keep logs with override)
  - CMM 92
- reset configuration (keep logs)
  - CMM 92
- reset default configuration 91
- reset network port settings
  - CMM 242
- responding to thermal events 144
- restart delay
  - set for compute node 259
  - set for I/O-module 259
- restore
  - configuration 269
  - permission groups 269
  - users 269
- restore CMM configuration command
  - example 273
- restore configuration
  - CMM (from file) 271
  - CMM (from file) and reset 272
- restore configuration (verbose)
  - CMM (from file) 271
- restore configuration (verbose) and reset

- CMM (from file) 273
- restore default configuration
  - CMM 91
- retry count
  - set for SOL 310
- retry interval
  - set for remote alerts 48
  - set for SOL 309
- retry limit
  - set for remote alerts 49
- revert to old IP address configuration after reset
  - I/O module 188
- room location
  - set for chassis 98
- RSA host key information
  - display for CMM 315
- Russia Class A electronic emission statement 470

## S

- save CMM configuration command
  - example 384
- save configuration to file
  - CMM 384
- save event log
  - CMM 117
- save service information
  - override warnings 118
  - with warnings 118
- scalable complex
  - display all information 280
  - display node information 281
  - display partition information 281
  - display specific complex information 280
- scale 280
  - options
    - compid 280
    - node 281
    - partid 281
- scale command errors 437
- scale commands 279
  - example 281
- scripting guidelines 1
- sddump
  - options
    - coll 285
    - init 285
- sddump command errors 437
- sddump commands 284
  - example 286
- sdemail
  - options
    - subj 287
    - to 287
- sdemail command errors 438
- sdemail commands 286
  - example 287
- search domain
  - set for Domain Catalog discovery 205
- secure command-line interface 16
- secure LDAP
  - disable 317
  - enable 317
- Secure Shell connection clients 17
- Secure Shell server
  - exit codes (CLI) 22
- secure TCP command mode
  - disable 335
  - disable for CMM 250, 342
  - enable 335
  - enable for CMM 250
  - set number of sessions 335

- turn secure TCP command mode on or off for the
  - CMM 250, 342
- secure TCP command mode port number
  - set for CMM 246
- security 16, 289
  - display CMM account settings 36
  - enable complex password for CMM user authentication 39
  - enable default administration password expiration for
    - CMM 40
  - enable password change at first login to CMM 42
  - options
    - p 289
  - set CMM account default to high 37
  - set CMM account default to legacy 36
  - set CMM account inactivity alert time 40
  - set CMM account inactivity disable time 41
  - set CMM account lockout period 42
  - set CMM authentication logging timeout 38
  - set CMM CLI inactivity timeout 39
  - set CMM maximum LDAP sessions for user 42
  - set CMM maximum number of login failures 41
  - set CMM minimum number of different characters for
    - password 40
  - set CMM password expiration time 43
  - set CMM password minimum change interval 43
  - set CMM password reuse cycle 44
  - set CMM user authentication method 39
  - set CMM web interface inactivity timeout 44
- security command errors 438
- security commands 287
  - account security 35
  - example 289
- security policy (chassis) 289
  - display CMM setting 289
- security policy, chassis 287
- selecting command environment 6
- selecting command target 6
- self-signed certificate
  - generate for certificate authority 319
  - view for CMM CA 318
- send threshold
  - set for SOL 310
- sending diagnostic data 462
- serial connection CMM 20
- Serial Over LAN 26
- Serial Over LAN commands 308
  - example 314
- serial port baud rate
  - set for CMM 238
- serial port communication rate
  - set for CMM 238
- serial port configuration
  - display for CMM 238
- serial port parity
  - set for CMM 239
- serial port settings for CMM commands
  - example 239
- serial port stop bits
  - set for CMM 239
- server host name
  - set for CMM 294
- server IP address
  - set for CMM 294
- service
  - options
    - hard 293
    - vr 291
    - vr, o 292
- Service Advisor
  - contact information 71
  - disable 71
  - display owner 70
  - enable 71
  - HTTP proxy setup 75
  - Service Advisor (alternate)

- contact information 73
- service and support
  - before you call 461
  - hardware 463
  - software 463
- service command
  - example 293
- service command errors 438
- service commands 290
- service data
  - collect for compute node 285
  - display command 118
  - dump from compute node 285
  - dump from I/O module 285
  - get for compute node 285
- service information
  - email 287
    - exclude from email alerts 49
    - include with email alerts 49
    - problem description 287
- service information (override warnings)
  - save 118
- service information (with warnings)
  - save 118
- service level reset 290
- service processor, user accounts 354
- set
  - date, CMM 107
  - global VLAN state 372
  - non-fixed VLAN state 373
  - power management policy 236
  - sol access (VLAN) 375
  - TCP command-mode session timeout 334
  - time zone, CMM 107
  - time, CMM 107
  - VLAN entry name 376
  - VLAN ID 375
  - VLAN IP address (IPv4) 377
  - VLAN IP address (IPv6) 379
  - VLAN IPv4 configuration method 376
  - VLAN IPv4 gateway 377
  - VLAN IPv4 prefix length 379
  - VLAN IPv4 subnet 377
  - VLAN IPv4 subnet mask 378
  - VLAN IPv4 subnet route 378
  - VLAN IPv6 configuration method 379
  - VLAN IPv6 gateway 380
  - VLAN IPv6 subnet prefix length 380
  - VLAN IPv6 subnet route 380
  - VLAN sol access 375
- set accumulate timeout
  - SOL 311
- set Active Directory group authority level 153
- set address prefix length
  - compute node 183
  - I/O module 190
- set alert notification method 55
- set alert recipient email address 55
- set alert recipient name 53
- set alert recipient status 53
- set alert type 54
- set automatic power-on policy
  - compute node 258
- set boot mode
  - compute node 65
- set chassis security policy
  - CMM 289
- set CIM port number
  - CMM 244
- set CIN state for disable
  - CMM 85
- set CIN state for enable
  - CMM 85
- set CLI key sequence
  - SOL 313
- set CMM account inactivity alert time 40
- set CMM account inactivity disable time 41
- set CMM account lockout period 42
- set CMM account security default
  - high 37
  - legacy 36
- set CMM authentication logging timeout 38
- set CMM CLI inactivity timeout 39
- set CMM maximum LDAP sessions for user 42
- set CMM maximum number of login failures 41
- set CMM minimum number of different characters for password 40
- set CMM password expiration time 43
- set CMM password minimum change interval 43
- set CMM password reuse cycle 44
- set CMM user authentication method 39
- set CMM web interface inactivity timeout 44
- set contact name
  - CMM 99
- set cryptographic settings
  - CMM 104
- set DNS first IPv4 IP address
  - CMM 121
- set DNS first IPv6 IP address
  - CMM 122
- set DNS second IPv4 IP address
  - CMM 122
- set DNS second IPv6 IP address
  - CMM 123
- set DNS server priority
  - CMM 123
- set DNS third IPv4 IP address
  - CMM 122
- set DNS third IPv6 IP address
  - CMM 123
- set Ethernet channel 0 address prefix length
  - CMM 176
- set Ethernet channel 0 data rate
  - CMM 173
- set Ethernet channel 0 domain name
  - CMM (primary) 175
  - CMM (standby) 176
- set Ethernet channel 0 duplex mode
  - CMM 173
- set Ethernet channel 0 floating IP address (IPv4)
  - CMM 168
- set Ethernet channel 0 floating IP address (IPv6)
  - CMM 168
- set Ethernet channel 0 gateway IP address (IPv4)
  - CMM 170
- set Ethernet channel 0 gateway/default route (IPv6)
  - CMM 170
- set Ethernet channel 0 hostname
  - CMM 171
  - standby CMM 172
- set Ethernet channel 0 IPv4 configuration method
  - CMM 172
- set Ethernet channel 0 MAC address
  - CMM (primary) 174
  - standby CMM 175
- set Ethernet channel 0 MTU
  - CMM 174
- set Ethernet channel 0 static IP address (IPv4)
  - CMM 166
  - standby CMM 169
- set Ethernet channel 0 static IP address (IPv6)
  - CMM 167
  - standby CMM 169
- set Ethernet channel 0 subnet mask (IPv4)
  - CMM 171
- set Ethernet-over-USB setting
  - compute node 130
- set first LDAP server host name
  - CMM 206
- set first LDAP server IP address

CMM 206  
 set first LDAP server port number  
   CMM 207  
 set for CMM 289  
 set fourth LDAP server host name  
   CMM 207  
 set fourth LDAP server IP address  
   CMM 207  
 set fourth LDAP server port number  
   CMM 208  
 set FTP data port number  
   CMM 243  
 set FTP port number  
   CMM 242  
 set FTP timeout  
   CMM 251  
 set gateway IP address (IPv4)  
   I/O module 187  
 set gateway IP address (IPv6)  
   I/O module 187  
 set hot air recirculation detection state (chassis) 143  
 set hot air recirculation threshold for chassis 143  
 set HTTP port number  
   CMM 243  
 set HTTPS port number  
   CMM 243  
 set IP address (IPv4)  
   CMM 166, 168  
   compute node 178  
   I/O module 186  
   standby CMM 169  
 set IP address (IPv6)  
   CMM 167–168  
   compute node 178  
   I/O module 187  
   standby CMM 169  
 set IPv4 network configuration method  
   I/O module 186  
 set LDAP client distinguished name  
   CMM 210  
 set LDAP client distinguished name password  
   CMM 210  
 set LDAP client distinguished name password (confirm)  
   CMM 210  
 set LDAP group filter  
   CMM 203  
 set LDAP group search attribute  
   CMM 203  
 set LDAP login permission attribute  
   CMM 204  
 set LDAP name  
   CMM 204  
 set LDAP security version  
   CMM 202  
 set LDAP server binding method  
   CMM 209  
 set LDAP server discovery method  
   CMM 205  
 set LDAP server domain name  
   CMM 205  
 set LDAP server for authentication only  
   CMM 209  
 set LDAP server forest name  
   CMM 205  
 set LDAP server root distinguished name  
   CMM 208  
 set LDAP UID search attribute  
   CMM 209  
 set location  
   CMM 99  
 set logical link loss alert and failover policy  
   CMM 352  
 set logical uplink failover delay  
   CMM 351  
 set logical uplink failover IP address  
   CMM 352  
 set logical uplink failover IPv6 IP address  
   CMM 352  
 set maximum number of simultaneous sessions for user 360  
 set name  
   chassis 96  
   CMM 96  
   compute node 97  
 set network interface gateway IP address (IPv4)  
   compute node 179  
 set network interface gateway/default route (IPv4)  
   compute node 180  
 set network interface IPv4 configuration method  
   compute node 181  
 set network interface static IP address (IPv4)  
   compute node 178  
 set network interface static IP address (IPv6)  
   compute node 178  
 set network interface subnet mask (IPv4)  
   compute node 181  
 set NTP server hostname  
   CMM 225  
 set NTP server IP address  
   CMM 225  
 set NTP server key  
   CMM 227  
 set NTP update frequency  
   CMM 226  
   I/O module 226  
 set number of sessions  
   secure TCP command mode 335  
   TCP command mode 335  
 set physical uplink failover delay  
   CMM 350  
 set port speed  
   switch 253  
 set power capping for compute node 145  
 set power domain redundancy loss policy 141  
 set rack location  
   chassis 97  
 set rack unit location  
   chassis 98  
 set reset compute node key sequence  
   SOL 313  
 set restart delay  
   compute node 259  
   I/O-module 259  
 set retry count  
   SOL 310  
 set retry interval  
   remote alerts 48  
   SOL 309  
 set retry limit  
   remote alerts 49  
 set room location  
   chassis 98  
 set second LDAP server host name  
   CMM 206  
 set second LDAP server IP address  
   CMM 206  
 set second LDAP server port number  
   CMM 207  
 set secure TCP command mode port number  
   CMM 246  
 set security policy (chassis)  
   CMM 289  
 set send threshold  
   SOL 310  
 set serial port baud rate  
   CMM 238  
 set serial port communication rate  
   CMM 238  
 set serial port parity  
   CMM 239  
 set serial port stop bits



CMM 239  
 set server host name  
   CMM 294  
 set server IP address  
   CMM 294  
 set SLP port number  
   CMM 244  
 set SMTP e-mail server domain name  
   CMM 294  
 set SNMP agent port number  
   CMM 244  
 set SNMP community 1 first host name  
   CMM 297  
 set SNMP community 1 first host name -get  
   CMM 299  
 set SNMP community 1 first host name to set  
   CMM 298  
 set SNMP community 1 IP address (first host)  
   CMM 297  
 set SNMP community 1 IP address (first host) to get  
   CMM 299  
 set SNMP community 1 IP address (first host) to set  
   CMM 298  
 set SNMP community 1 IP address (second host)  
   CMM 299  
 set SNMP community 1 IP address (third host)  
   CMM 300  
 set SNMP community 1 name  
   CMM 297  
 set SNMP community 1 second host name  
   CMM 299  
 set SNMP community 1 third host name  
   CMM 300  
 set SNMP community 1 view type (SNMPv3)  
   CMM 300  
 set SNMP community 2 first host name  
   CMM 301  
 set SNMP community 2 IP address (first host)  
   CMM 301  
 set SNMP community 2 IP address (second host)  
   CMM 302  
 set SNMP community 2 IP address (third host)  
   CMM 303  
 set SNMP community 2 name  
   CMM 301  
 set SNMP community 2 second host name  
   CMM 302  
 set SNMP community 2 third host name  
   CMM 303  
 set SNMP community 2 view type (SNMPv3)  
   CMM 303  
 set SNMP community 3 first host name  
   CMM 304  
 set SNMP community 3 IP address (first host)  
   CMM 304  
 set SNMP community 3 IP address (second host)  
   CMM 305  
 set SNMP community 3 IP address (third host)  
   CMM 306  
 set SNMP community 3 name  
   CMM 304  
 set SNMP community 3 second host name  
   CMM 305  
 set SNMP community 3 third host name  
   CMM 306  
 set SNMP community 3 view type (SNMPv3)  
   CMM 306  
 set SNMP contact name  
   CMM 307  
 set SNMP location  
   CMM 307  
 set SNMP traps port number  
   CMM 245  
 set SSH port number  
   CMM 246  
 set state  
   VLAN tagging 376  
 set static power limit for chassis 144  
 set subnet mask (IPv4)  
   I/O module 188  
 set syslog event log collector 1 host name  
   CMM 330  
 set syslog event log collector 1 IP address  
   CMM 330  
 set syslog event log collector 1 port number  
   CMM 331  
 set syslog event log collector 2 host name  
   CMM 331  
 set syslog event log collector 2 IP address  
   CMM 331  
 set syslog event log collector 2 port number  
   CMM 332  
 set syslog filter level  
   CMM 329  
 set TCP command mode port number  
   CMM 245  
 set TCP command-mode timeout  
   CMM 251  
 set Telnet port number  
   CMM 246  
 set Telnet port timeout  
   CMM 252  
 set TFTP port number  
   CMM 247  
 set third LDAP server host name  
   CMM 206  
 set third LDAP server IP address  
   CMM 206  
 set third LDAP server port number  
   CMM 208  
 set trespass feature message  
   CMM 338  
 set trespass feature to default  
   CMM 338  
 set user permission groups 359  
 SFTP  
   disable for CMM 247  
   enable for CMM 247  
 SFTP status  
   display for CMM 315  
 shutdown  
   compute node 256  
 simultaneous sessions  
   set maximum number for user 360  
 SLP  
   disable for CMM 248  
   enable for CMM 248  
 SLP port number  
   set for CMM 244  
 SMS  
   disable for compute node 255  
   enable for compute node 255  
 smtp 294  
   options  
     d 294  
     s 294  
 smtp command errors 439  
 smtp commands 293  
   example 295  
 SMTP e-mail server domain name  
   set for CMM 294  
 SMTP server host name  
   display for CMM 294  
 SMTP server IP address  
   display for CMM 294  
 SMTP settings for CMM commands  
   example 295  
 snmp 296  
   options  
     -ca1 get -c1i1 0.0.0.0 299

- ca1 set -c1i1 0.0.0.0 298
- a, on 296
- a3, on 296
- c1 297
- c1i1 297
- c1i2 299
- c1i3 300
- c2 301
- c2i1 301
- c2i2 302
- c2i3 303
- c3 304
- c3i1 304
- c3i2 305
- c3i3 306
- ca1 300
- ca2 303
- ca3 306
- cn 307
- l 307
- t, on 296
- SNMP agent
  - enable for CMM (SNMPv1)
    - SNMPv1 296
  - enable for CMM (SNMPv3)
    - SNMPv3 296
- SNMP agent port number
  - set for CMM 244
- snmp command errors 440
- snmp commands 295
  - example 308
- SNMP community 1 first host name
  - set for CMM 297
  - set to get for CMM 299
- SNMP community 1 first host name to set
  - set for CMM 298
- SNMP community 1 IP address (first host)
  - set for CMM 297
- SNMP community 1 IP address (first host) to get
  - set to get for CMM 299
- SNMP community 1 IP address (first host) to set
  - set for CMM 298
- SNMP community 1 IP address (second host)
  - set for CMM 299
- SNMP community 1 IP address (third host)
  - set for CMM 300
- SNMP community 1 name
  - set for CMM 297
- SNMP community 1 second host name
  - set for CMM 299
- SNMP community 1 third host name
  - set for CMM 300
- SNMP community 1 view type
  - set for CMM (SNMPv3) 300
- SNMP community 2 first host name
  - set for CMM 301
- SNMP community 2 IP address (first host)
  - set for CMM 301
- SNMP community 2 IP address (second host)
  - set for CMM 302
- SNMP community 2 IP address (third host)
  - set for CMM 303
- SNMP community 2 name
  - set for CMM 301
- SNMP community 2 second host name
  - set for CMM 302
- SNMP community 2 third host name
  - set for CMM 303
- SNMP community 2 view type
  - set for CMM (SNMPv3) 303
- SNMP community 3 first host name
  - set for CMM 304
- SNMP community 3 IP address (first host)
  - set for CMM 304
- SNMP community 3 IP address (second host)
  - set for CMM 305
- SNMP community 3 IP address (third host)
  - set for CMM 306
- SNMP community 3 name
  - set for CMM 304
- SNMP community 3 second host name
  - set for CMM 305
- SNMP community 3 third host name
  - set for CMM 306
- SNMP community 3 view type
  - set for CMM (SNMPv3) 306
- SNMP configuration
  - display for CMM 296
- SNMP contact name
  - set for CMM 307
- SNMP location
  - set for CMM 307
- SNMP settings for CMM commands
  - example 308
- SNMP traps
  - disable for CMM 249, 296
  - enable for CMM 249, 296
- SNMP traps port number
  - set for CMM 245
- SNMPv1
  - disable for CMM 341
  - enable for CMM 341
- SNMPv1 agent
  - disable for CMM 249
  - enable for CMM 249
- SNMPv3
  - community 1 view type 300
  - community 2 view type 303
  - community 3 view type 306
  - disable for CMM 341
  - enable for CMM 341
- SNMPv3 agent
  - disable for CMM 249
  - enable for CMM 249
- SNMPv3 centralized user account management
  - disable for CMM 367
  - disable for compute nodes 366
  - enable for CMM 367
  - enable for compute nodes 366
- SNMPv3 information
  - update for user 365
- software service and support telephone numbers 463
- sol 309
  - options
    - c 310
    - e 313
    - i 309
    - r 313
    - s 310
    - status 311–312
    - t 311
- SOL 26, 100
  - global disable 312
  - global enable 311
  - set accumulate timeout 311
  - set CLI key sequence 313
  - set reset compute node key sequence 313
  - set retry count 310
  - set retry interval 309
  - set send threshold 310
  - status 309
- sol access (VLAN)
  - disable 375
  - enable 375
  - set 375
- sol command errors 440
- sol commands
  - example 314
- SOL commands 308
- SOL session

- ending 27, 100
- starting 26
- Specify IP address
  - CIN configuration entry 88
- Specify VLAN ID
  - CIN configuration 88
- SSH
  - using 22
- SSH clients 17
- SSH connectionCMM 21
- SSH port
  - disable for CMM 249
  - enable for CMM 249
- SSH port number
  - set for CMM 246
- SSH public key
  - add for user 361
  - display 363
  - display complete 363
  - download 363
  - export 363
  - import (add) 362
  - import (update) 362
  - remove from user 361
  - update 364
  - upload (add) 362
  - upload (update) 362
- SSH status
  - display for CMM 315
- sshcfg 315
  - options
    - cstatus 316
    - hk, dsa 315
    - hk, gen 316
    - hk, rsa 315
    - sftpstatus 316
- sshcfg command 315
  - example 316
- sshcfg command errors 442
- SSL
  - disable for HTTPS server 318
  - disable for LDAP client 317
  - enable for HTTPS server 318
  - enable for LDAP client 317
- SSL certificate
  - download certificate file (format) 322
- SSL certificate status
  - CMM 317
- SSL CSR
  - download certificate file (format) 322
- SSL for HTTPS server
  - disable 318
  - enable 318
- SSL for LDAP client
  - disable 317
  - enable 317
- SSL status
  - CMM 317
- sslcfg 317
  - f 322
  - options
    - c 319
    - cl 319
    - client 317
    - cp 319
    - cpwd 319
    - csa 319
    - dnld 321–322
    - download 324–325
    - dq 319
    - ea 319
    - gen, ca 319
    - gen, csr 319
    - gn 319
    - hn 319
    - i 322–324
    - in 319
    - on 319
    - ou 319
    - remove 326–327
    - s 319
    - server 318
    - sp 319
    - t 319, 322–327
    - tc1 322, 324, 326
    - tc2 323, 325–326
    - tc3 324–325, 327
    - u 321–325
    - un 319
    - upld, u 327
    - view, ca 318
  - t 321–322
- sslcfg command errors 442
- sslcfg commands 317
  - example 327
- standby CMM
  - set Ethernet channel 0 hostname 172
  - set Ethernet channel 0 MAC address 175
  - set Ethernet channel 0 static IP address (IPv4) 169
  - set Ethernet channel 0 static IP address (IPv6) 169
  - set IP address (IPv4) 169
  - set IP address (IPv6) 169
- standby CMMs 8
- starting a session using Telnet 19
- starting an SOL session 26
- starting command-line interface 16
- state
  - disable for VLAN (global) 372
  - disable for VLAN (non-fixed) 373
  - enable for VLAN (global) 372
  - enable for VLAN (non-fixed) 373
  - set for VLAN (global) 372
  - set for VLAN (non-fixed) 373
- static IP address (IPv4)
  - set for channel 0 of CMM 166
  - set for channel 0 of standby CMM 169
  - set for network interface of compute node 178
- static IP address (IPv6)
  - set for channel 0 of CMM 167
  - set for channel 0 of standby CMM 169
  - set for network interface of compute node 178
- static IPv6 configuration
  - disable for CMM 176
  - disable for I/O module 190
  - enable for CMM 176
  - enable for I/O module 190
- static power limit, set for chassis 144
- status
  - display for CIM subscriptions 82
  - display for CMM 118
  - SOL 309
- stop bits
  - set for serial port of CMM 239
- storage backplane
  - command target 126
- storage DIMM, flash 7, 126
- storage expansion enclosure
  - command target 128
- subnet mask (IPv4)
  - set for channel 0 of CMM 171
  - set for I/O module 188
  - set for network interface of compute node 181
- subscription
  - CIM 81
  - common information model 81
- support web page, custom 462
- switch
  - disable port 253
  - display network port settings 252
  - enable port 253

- set port speed 253
- switch module
  - command target 127
  - cycle power 256
  - display POST status 259
  - display power state 257
  - power off 256
  - power on 255–256
  - reset 277
  - reset (extended diagnostics) 279
  - reset (full diagnostics) 279
  - reset (standard diagnostics) 278
  - reset configuration 93
  - turn off 256
  - turn on 255–256
- synchronize clock with NTP server
  - CMM 227
- syntax help 160
- syntax help commands
  - example 161
- syslog 329
  - options
    - coll1 329
    - coll2 330
    - i1 330
    - i2 331
    - p1 331
    - p2 332
    - sev 329
    - test 332
- syslog command errors 444
- syslog commands 328
  - example 333
- syslog configuration
  - display for CMM 329
- syslog event log collector 1 host name
  - set for CMM 330
- syslog event log collector 1 IP address
  - set for CMM 330
- syslog event log collector 1 port number
  - set for CMM 331
- syslog event log collector 2 host name
  - set for CMM 331
- syslog event log collector 2 IP address
  - set for CMM 331
- syslog event log collector 2 port number
  - set for CMM 332
- syslog event log transmission for collector 1
  - disable 329
  - disable for CMM 329
  - enable 329
  - enable for CMM 329
- syslog event log transmission for collector 2
  - disable 330
  - disable for CMM 330
  - enable 330
  - enable for CMM 330
- syslog filter level
  - set for CMM 329
- syslog test message
  - generate for CMM 332
- system
  - view configuration tree 214
- system physical configuration command 214
- system power management policy command 235
- system-management processor
  - command target 126
  - reset 277
- system, display power trending 142
- Taiwan product service 463
- target 35, 124
- TCP command mode
  - disable 334
  - disable for CMM 250, 341
  - enable 335
  - enable for CMM 250
  - set number of sessions 335
  - turn TCP command mode on or off for the CMM 250, 341
- TCP command mode port number
  - set for CMM 245
- TCP command-mode session status
  - display 334
- TCP command-mode session timeout
  - display 334
  - set 334
- TCP command-mode timeout
  - set for CMM 251
- tcpcmdmode 334
  - options
    - sstatus, 0 335
    - sstatus, 1 to 20 335
    - status, 0 334
    - status, 1 to 20 335
    - t 334
- tcpcmdmode command errors 445
- tcpcmdmode commands 333
  - example 336
- telecommunication regulatory statement 467
- telephone numbers 463
- Telnet connection 16, 19
- Telnet port
  - disable for CMM 250
  - enable for CMM 250
- Telnet port number
  - set for CMM 246
- Telnet port timeout
  - set for CMM 252
- temperature
  - display for CMM 336
  - display for compute node 336
  - display for front panel card 336
- temperature display, fan module 140
- temperature display, rear LED card 140
- temporary command target 7
- temps 336
- temps command errors 446
- temps commands 336
  - example 336
- terminate 355
- terminate session 133
- terminate user session
  - CMM 355
- test alert
  - generate 56
- test call home
  - call-home 80
- test communication
  - compute node IP address 234
  - I/O-module IP address 234
  - IP address (compute node) 233–234
  - IP address (I/O module) 233
  - IP address (I/O-module) 234
- TFTP
  - disable for CMM 251
  - enable for CMM 251
- TFTP port number
  - set for CMM 247
- thermal event response 144
- thermal trending, display (fan module) 142
- thermal trending, display (rear LED card) 142
- time
  - display for CMM 106
  - set for CMM 107
- time zone

## T

Taiwan Class A electronic emission statement 470

- set for CMM 107
- timezone
  - display valid settings 106
  - display valid settings (verbose) 106
- trademarks 466
- trespass 337
  - options
    - tw 338
    - twd 338
    - twe 337
- trespass command 337
  - example 339
- trespass command errors 446
- trespass feature
  - enable for CMM 337
- trespass feature default
  - set for CMM 338
- trespass feature message
  - set for CMM 338
- trespass feature status
  - display for CMM 337
- trusted certificate 1 (LDAP)
  - download 324
  - export 324
  - import 322
  - remove 326
  - upload 322
- trusted certificate 2 (LDAP)
  - download 325
  - export 325
  - import 323
  - remove 326
  - upload 323
- trusted certificate 3 (LDAP)
  - download 325
  - export 325
  - import 324
  - remove 327
  - upload 324
- turn all CIN index entries on or off 86
- turn off
  - compute node 256
  - I/O module 256
  - switch module 256
- turn off identify LED 213
- turn off LED
  - information 213
- turn on
  - compute node 255–256
  - I/O module 255–256
  - switch module 255–256
- turn on (to console)
  - compute node 255–256
- turn secure TCP command mode on or off
  - CMM 250, 342
- turn TCP command mode on or off
  - CMM 250, 341

## U

- uicfg 340
  - options
    - cim 340
    - cli 340
    - snmp, enabled 341
    - stcm, port mode 342
    - tcm, port mode 341
    - web, enabled 342
- uicfg command errors 446
- uicfg commands 339
  - example 342
- unacknowledge call-home activity log entry
  - CMM 78

- United States FCC Class A notice 468
- unlock user 356
- update
  - options
    - a 344
    - activate 348
    - u 344
    - u, img 346–347
    - u, img, activate 348
    - u, r 345
    - u, v 346
  - user SNMPv3 information 365
- update command 343
- update command errors 447
- update commands
  - example 349
- update firmware 343–345
  - I/O module 346–348
  - switch 346–348
  - verbose 347
- update firmware (verbose) 346
- update SSH public key 364
- uplink 350
  - options
    - alert 352
    - dls 351
    - dps 350
    - el, enabled 351
    - ep 350
    - ip 352
    - ip6 352
- uplink command errors 451
- uplink commands 349
  - example 353
- uplink configuration
  - display for CMM 350
- uplink failover (logical)
  - disable for CMM 351
  - enable for CMM 351
- uplink failover (physical)
  - enable for CMM 350
- uplink failover delay (logical)
  - set for CMM 351
- uplink failover delay (physical)
  - set for CMM 350
- uplink failover IP address (logical)
  - set for CMM 352
- uplink failover IPv6 IP address (logical)
  - set for CMM 352
- upload
  - certificate 327
  - LDAP trusted certificate 1 322
  - LDAP trusted certificate 2 323
  - LDAP trusted certificate 3 324
  - upload (add) SSH public key 362
  - upload (update) SSH public key 362
- URL
  - specifying 27
- user account management (centralized)
  - disable 138
- user accounts
  - IMM 354
  - service processor 354
- user authentication method
  - enable complex password 39
  - set for CMM 39
- user interface configuration 339
  - example 342
- user interface settings
  - display for CMM 340
- user permission group CMM 228
- user permission group, add 229
- user permission group, change 230
- user permission group, delete 231
- user permission group, modify 230

- user permission groups, display (all) 228
- user permission groups, display (specific) 228
- user session 355
- user SNMPv3 information
  - update 365
- users 354
  - backup 383
  - options
    - add 357, 361
    - af 364
    - am 366
    - ap 365
    - at 365
    - clear, n 356
    - cm 364
    - cn 365
    - curr 354
    - disable 355
    - dnld 363
    - enable 356
    - g 357, 359
    - i 365
    - ipmisnmpv3 367
    - ms 357, 360
    - n 355, 357
    - op 358
    - p 357–359
    - pp 365
    - ppw 365
    - remove 361
    - ts 355
    - u, ki 363
    - u, ki, e 363
    - unlock 356
    - upld 362
  - restore 269
  - users command 353
  - users command errors 452
  - users commands
    - example 367
  - users, add 357
  - users, add SSH public key 361
  - users, change password (other user) 359
  - users, change password (own password) 358
  - users, CMM 353
  - users, create 357
  - users, delete 356
  - users, disable 355
  - users, display (active) 354
  - users, display (all) 354
  - users, display (single) 355
  - users, enable 356
  - users, remove SSH public key 361
  - users, set maximum number of simultaneous sessions 360
  - users, set permission groups 359
  - users, unlock 356
- using
  - SSH 22
- using the command-line interface 5

## V

- V3 authentication for NTP
  - enable for CMM 226
- view
  - self-signed certificate (CMM CA) 318
- view command target 214
- virtual reset 290
  - CMM 291
  - compute node 291
  - I/O module 291
- virtual reset (suppress warnings)
  - CMM 292

- virtual reset 290
- vlan 371
  - c 376
  - c6 379
  - commit 371
  - cto 372
  - delete 373–374
  - g 377
  - g6 380
  - i 377
  - i6 379
  - n 376
  - p6 379
  - s 377
  - smx 378
  - sol 375
  - sp6x 380
  - sr6x 380
  - srx 378
  - state 372–373
  - tag 376
  - vi 371, 374
  - vid 375
- VLAN
  - disable (global) 372
  - disable (non-fixed) 373
  - display all settings 371
  - display settings for ID 371
  - enable (global) 372
  - enable (non-fixed) 373
  - state set (global) 372
  - state set (non-fixed) 373
- vlan command errors 456
- vlan commands 371
  - example 381
- VLAN commit timeout 372
- VLAN entry
  - create 374
  - delete all (non-fixed) 373
  - delete specific 374
- VLAN entry name
  - set 376
- VLAN ID
  - CIN configuration 88
  - set 375
- VLAN IP address
  - set (IPv4) 377
  - set (IPv6) 379
- VLAN IPv4 configuration method
  - set 376
- VLAN IPv4 gateway
  - set 377
- VLAN IPv4 prefix length
  - set 379
- VLAN IPv4 subnet
  - set 377
- VLAN IPv4 subnet mask
  - set 378
- VLAN IPv4 subnet route
  - set 378
- VLAN IPv6 configuration method
  - set 379
- VLAN IPv6 gateway
  - set 380
- VLAN IPv6 subnet prefix length
  - set 380
- VLAN IPv6 subnet route
  - set 380
- VLAN settings (CMM)
  - commit 371
- VLAN sol access
  - disable 375
  - enable 375
  - set 375
- VLAN tagging

- disable 376
- enable 376
- set state 376
- voltage
  - display for compute node 383
- volts 383
- volts command errors 459
- volts commands 382
  - example 383

## W

- Wake on LAN
  - enable for compute node 257
  - enable globally 257
- warning alerts
  - disable monitoring for all 218
  - disable monitoring for chassis 219
  - disable monitoring for cooling device 220
  - disable monitoring for event log 219
  - disable monitoring for I/O module 219
  - disable monitoring for node device 218
  - disable monitoring for power supply 220

- disable monitoring for system management 219
- enable monitoring for all 218
- enable monitoring for chassis 219
- enable monitoring for cooling device 220
- enable monitoring for event log 219
- enable monitoring for I/O module 219
- enable monitoring for node device 218
- enable monitoring for power supply 220
- enable monitoring for system management 219
- web interface
  - CA authentication 28
  - certificate authentication 28
  - CSR authentication 28
  - disable for CMM 342
  - enable for CMM 342
- web interface inactivity timeout
  - set for CMM 44
- write
  - options
    - u, p 384
- write command 383
  - example 384
- write command errors 459









Part Number: SP47A31813

Printed in China

(1P) P/N: SP47A31813

