Abstract
This guide details using the command-line interface for configuration, operation, and management of the HP BladeSystem Onboard Administrator 4.50 (or later) and the enclosure Insight Display.
## Contents

- **Introduction** ................................................................................................................................ 12
  - Overview of the Onboard Administrator .................................................................................... 12
  - CLI command categories ............................................................................................................. 12
  - What's new ................................................................................................................................. 13

- **Accessing the command line interface** ....................................................................................... 14
  - Remote access to the Onboard Administrator ............................................................................. 14
  - Local access to the Onboard Administrator .............................................................................. 14

- **Command line** ............................................................................................................................ 16
  - Command line overview .............................................................................................................. 16
  - Command line conventions ........................................................................................................ 16
    - Reserved words ....................................................................................................................... 16
  - HP Integrity server blade restrictions ........................................................................................... 17
  - Access level and privileges ........................................................................................................ 17
    - Account authentication .......................................................................................................... 19
    - AutoLogin to iLO .................................................................................................................. 19
  - CLEAR SCREEN ......................................................................................................................... 21
  - EXIT ............................................................................................................................................ 21
  - HELP .......................................................................................................................................... 21
  - LOGOUT ..................................................................................................................................... 21
  - QUIT .......................................................................................................................................... 22

- **Rack commands** ........................................................................................................................ 23
  - SET RACK NAME ...................................................................................................................... 23
  - SHOW RACK INFO .................................................................................................................... 24
  - SHOW RACK NAME ................................................................................................................... 24
  - SHOW TOPOLOGY ....................................................................................................................... 24

- **User account commands** ......................................................................................................... 26
  - ADD USER ................................................................................................................................. 26
  - ASSIGN .................................................................................................................................... 26
  - ASSIGN OA ............................................................................................................................... 27
  - DISABLE USER ......................................................................................................................... 27
  - DISABLE STRONG PASSWORDS .............................................................................................. 27
  - ENABLE STRONG PASSWORDS .............................................................................................. 28
  - ENABLE USER ......................................................................................................................... 28
  - HISTORY .................................................................................................................................. 28
  - REMOVE USER ....................................................................................................................... 29
  - SET MINIMUM PASSWORD LENGTH ....................................................................................... 29
  - SET PASSWORD ....................................................................................................................... 29
  - SET SESSION TIMEOUT ............................................................................................................ 30
  - SET USER ACCESS .................................................................................................................. 30
  - SET USER CONTACT ............................................................................................................... 30
  - SET USER FULLNAME ............................................................................................................. 31
  - SET USER PASSWORD .............................................................................................................. 31
SHOW PASSWORD SETTINGS ................................................................. 32
SHOW SESSION TIMEOUT ................................................................. 32
SHOW USER .................................................................................... 33
SLEEP ............................................................................................ 33
UNASSIGN .................................................................................... 33
UNASSIGN OA .............................................................................. 34

Two-Factor Authentication commands ............................................. 35
ADD CA CERTIFICATE ..................................................................... 35
DISABLE CRL ................................................................................. 35
DISABLE TWOFACTOR .................................................................. 36
DOWNLOAD CA CERTIFICATE ....................................................... 36
DOWNLOAD USER CERTIFICATE .................................................... 36
REMOVE CA CERTIFICATE ............................................................. 37
REMOVE USER CERTIFICATE ........................................................ 37
SET USER CERTIFICATE ............................................................... 37
SHOW CA CERTIFICATES ............................................................... 38
SHOW TWOFACTOR INFO ............................................................... 39

Directory commands ....................................................................... 40
ADD LDAP CERTIFICATE ............................................................... 40
ADD LDAP GROUP ........................................................................ 40
ASSIGN for LDAP ......................................................................... 41
ASSIGN OA LDAP GROUP ............................................................. 41
DISABLE LDAP ............................................................................. 41
DOWNLOAD LDAP CERTIFICATE .................................................. 42
ENABLE LDAP ............................................................................... 42
REMOVE LDAP CERTIFICATE ....................................................... 42
REMOVE LDAP GROUP ................................................................. 43
SET LDAP GROUP ACCESS .......................................................... 43
SET LDAP GROUP DESCRIPTION ................................................ 43
SET LDAP NAME MAP .................................................................. 44
SET LDAP GCPORT ...................................................................... 44
SET LDAP PORT .......................................................................... 44
SET LDAP SEARCH ...................................................................... 45
SET LDAP SERVER ....................................................................... 45
SHOW LDAP CERTIFICATE ........................................................... 45
SHOW LDAP GROUP .................................................................... 46
SHOW LDAP INFO ........................................................................ 46
TEST LDAP .................................................................................. 47
UNASSIGN for LDAP ................................................................. 47
UNASSIGN OA LDAP GROUP ....................................................... 47

HP SIM commands ......................................................................... 49
ADD HPSIM CERTIFICATE ............................................................. 49
DOWNLOAD HPSIM CERTIFICATE ................................................ 49
REMOVE HPSIM CERTIFICATE ..................................................... 50
SET HPSIM TRUST MODE ............................................................ 50
SHOW HPSIM INFO ...................................................................... 50

General management commands .................................................. 52
DISABLE URB ................................................................................. 52
DOWNLOAD OA CERTIFICATE ....................................................... 52
ENABLE URB ............................................................................... 53
FORCE TAKEOVER ....................................................................... 53
Enclosure Bay IP Addressing commands ................................................................. 61
ADD EBIPA....................................................................................................................... 61
ADD EBIPAV6 .................................................................................................................... 61
DISABLE EBIPA .................................................................................................................. 61
DISABLE EBIPAV6 .............................................................................................................. 62
ENABLE EBIPA ................................................................................................................... 62
ENABLE EBIPAV6 .............................................................................................................. 63
REMOVE EBIPA .................................................................................................................. 63
REMOVE EBIPAV6 .............................................................................................................. 64
SAVE EBIPA ........................................................................................................................ 64
SAVE EBIPAV6 ................................................................................................................... 65
SET EBIPA INTERCONNECT ............................................................................................... 65
SET EBIPA SERVER ............................................................................................................ 66
SET EBIPAV6 INTERCONNECT ............................................................................................ 67
SET EBIPAV6 SERVER ........................................................................................................ 68
SHOW EBIPA ..................................................................................................................... 70
SHOW EBIPAV6 ................................................................................................................ 73

Enclosure network configuration commands .............................................................. 77
ADD OA ADDRESS IPV6 .................................................................................................... 77
ADD OA DNS ....................................................................................................................... 77
ADD OA DNS IPV6 ............................................................................................................ 78
ADD OA ROUTE IPV6 ....................................................................................................... 79
ADD SSHKEY ..................................................................................................................... 79
ADD SNMP TRAPRECEIVER ........................................................................................... 80
ADD SNMP TRAPRECEIVER V3 ..................................................................................... 81
ADD SNMP USER ............................................................................................................... 82
ADD TRUSTED HOST ......................................................................................................... 83
CLEAR LOGIN_BANNER_TEXT ......................................................................................... 84
CLEAR NTP .......................................................................................................................... 84
CLEAR SSHKEY ................................................................................................................ 84
CLEAR VCMODE ............................................................................................................... 84
DISABLE ALERTMAIL ....................................................................................................... 85
DISABLE DHCPV6 ............................................................................................................. 85
DISABLE ENCLOSURE_ILO_FEDERATION_SUPPORT ......................................................... 85
DISABLE ENCLOSURE_IP_MODE ....................................................................................... 86
DISABLE HTTPS ............................................................................................................... 86
DISABLE FQDN_LINK_SUPPORT ....................................................................................... 86
DISABLE IPV6 .................................................................................................................... 87
DISABLE IPV6DYNDNS ..................................................................................................... 87
DISABLE LOGIN_BANNER ............................................................................................... 88
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blade management commands</td>
<td>168</td>
</tr>
<tr>
<td>ASSIGN SERVER</td>
<td>168</td>
</tr>
<tr>
<td>CONNECT SERVER</td>
<td>168</td>
</tr>
<tr>
<td>HPONCFG</td>
<td>168</td>
</tr>
<tr>
<td>POWEROFF SERVER</td>
<td>170</td>
</tr>
<tr>
<td>POWERON SERVER</td>
<td>170</td>
</tr>
<tr>
<td>REBOOT SERVER</td>
<td>171</td>
</tr>
<tr>
<td>Enclosure Firmware Management commands</td>
<td>157</td>
</tr>
<tr>
<td>CLEAR FIRMWARE MANAGEMENT ALL_LOGS</td>
<td>157</td>
</tr>
<tr>
<td>DISCOVER FIRMWARE SERVER</td>
<td>157</td>
</tr>
<tr>
<td>DISABLE FIRMWARE MANAGEMENT</td>
<td>157</td>
</tr>
<tr>
<td>ENABLE FIRMWARE MANAGEMENT</td>
<td>158</td>
</tr>
<tr>
<td>SET FIRMWARE MANAGEMENT</td>
<td>158</td>
</tr>
<tr>
<td>SET FIRMWARE MANAGEMENT URL</td>
<td>158</td>
</tr>
<tr>
<td>SET FIRMWARE MANAGEMENT POLICY</td>
<td>159</td>
</tr>
<tr>
<td>SET FIRMWARE MANAGEMENT POWER</td>
<td>159</td>
</tr>
<tr>
<td>SET FIRMWARE MANAGEMENT SCHEDULE</td>
<td>160</td>
</tr>
<tr>
<td>SET FIRMWARE MANAGEMENT BAYS_TO_INCLUDE SERVER</td>
<td>160</td>
</tr>
<tr>
<td>SET FIRMWARE MANAGEMENT FORCE_DOWNGRADE</td>
<td>160</td>
</tr>
<tr>
<td>SHOW FIRMWARE</td>
<td>161</td>
</tr>
<tr>
<td>SHOW FIRMWARE MANAGEMENT</td>
<td>161</td>
</tr>
<tr>
<td>SHOW FIRMWARE MANAGEMENT LOG</td>
<td>162</td>
</tr>
<tr>
<td>SHOW FIRMWARE SUMMARY</td>
<td>162</td>
</tr>
<tr>
<td>SHOW FIRMWARE SUMMARY CSV</td>
<td>164</td>
</tr>
<tr>
<td>SHOW FIRMWARE LOG SERVER</td>
<td>165</td>
</tr>
<tr>
<td>SHOW FIRMWARE LOG SESSION</td>
<td>165</td>
</tr>
<tr>
<td>SHOW FIRMWARE SERVER</td>
<td>166</td>
</tr>
<tr>
<td>UPDATE FIRMWARE SERVER</td>
<td>166</td>
</tr>
<tr>
<td>Blade management commands</td>
<td>168</td>
</tr>
<tr>
<td>ASSIGNED SERVER</td>
<td>168</td>
</tr>
<tr>
<td>CONNECT SERVER</td>
<td>168</td>
</tr>
<tr>
<td>HPONCFG</td>
<td>168</td>
</tr>
<tr>
<td>POWEROFF SERVER</td>
<td>170</td>
</tr>
<tr>
<td>POWERON SERVER</td>
<td>170</td>
</tr>
<tr>
<td>REBOOT SERVER</td>
<td>171</td>
</tr>
<tr>
<td>Command</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>SET NIC</td>
<td>171</td>
</tr>
<tr>
<td>SET SERVER BOOT</td>
<td>172</td>
</tr>
<tr>
<td>SET SERVER BOOT FIRST</td>
<td>172</td>
</tr>
<tr>
<td>SET SERVER BOOT ONCE</td>
<td>173</td>
</tr>
<tr>
<td>SET SERVER POWERDELAY</td>
<td>174</td>
</tr>
<tr>
<td>SET SERVER UID</td>
<td>174</td>
</tr>
<tr>
<td>SHOW SERVER BOOT</td>
<td>174</td>
</tr>
<tr>
<td>SHOW SERVER INFO</td>
<td>175</td>
</tr>
<tr>
<td>SHOW SERVER LIST</td>
<td>177</td>
</tr>
<tr>
<td>SHOW SERVER NAMES</td>
<td>178</td>
</tr>
<tr>
<td>SHOW SERVER PORT MAP</td>
<td>179</td>
</tr>
<tr>
<td>SHOW SERVER POWERDELAY</td>
<td>180</td>
</tr>
<tr>
<td>SHOW SERVER STATUS</td>
<td>181</td>
</tr>
<tr>
<td>SHOW SERVER TEMP</td>
<td>183</td>
</tr>
<tr>
<td>SHOW SYSLOG SERVER</td>
<td>184</td>
</tr>
<tr>
<td>UNASSIGN SERVER</td>
<td>185</td>
</tr>
<tr>
<td>DOWNLOAD CONFIG using USB key</td>
<td>204</td>
</tr>
<tr>
<td>TEST SYSLOG</td>
<td>202</td>
</tr>
<tr>
<td>SHOW SYSLOG SETTINGS</td>
<td>202</td>
</tr>
<tr>
<td>SET REMOTE SYSLOG PORT</td>
<td>201</td>
</tr>
<tr>
<td>SHOW SYSLOG SETTINGS</td>
<td>202</td>
</tr>
<tr>
<td>SHOW SYSLOG SETTINGS</td>
<td>202</td>
</tr>
<tr>
<td>TEST SYSLOG</td>
<td>202</td>
</tr>
<tr>
<td>Remote syslog example</td>
<td>203</td>
</tr>
<tr>
<td>USB support commands</td>
<td>204</td>
</tr>
<tr>
<td>USB support commands</td>
<td>204</td>
</tr>
</tbody>
</table>

**Interconnect management commands**

- ASSIGN INTERCONNECT
- CLEAR INTERCONNECT SESSION
- CONNECT INTERCONNECT
- POWEROFF INTERCONNECT
- POWERON INTERCONNECT
- RESTART INTERCONNECT
- SET INTERCONNECT ADMIN_PASSWORD FACTORY
- SET INTERCONNECT FACTORY
- SET INTERCONNECT POWERDELAY
- SET INTERCONNECT UID
- SHOW INTERCONNECT
- SHOW INTERCONNECT INFO
- SHOW INTERCONNECT LIST
- SHOW INTERCONNECT PORT MAP
- SHOW INTERCONNECT POWERDELAY
- SHOW INTERCONNECT SESSIONS
- SHOW INTERCONNECT STATUS

**Active Health System commands**

- ENABLE ACTIVE HEALTH SYSTEM
- DISABLE ACTIVE HEALTH SYSTEM

**Enclosure DVD commands**

- SET Server DVD
- SHOW Server DVD

**Remote syslog commands**

- DISABLE SYSLOG REMOTE
- ENABLE SYSLOG REMOTE
- SET REMOTE SYSLOG PORT
- SET REMOTE SYSLOG SERVER
- SHOW SYSLOG SETTINGS
- TEST SYSLOG

**USB support commands**

- DOWNLOAD CONFIG using USB key
Introduction

Overview of the Onboard Administrator

The HP BladeSystem Onboard Administrator is the intelligence of the HP BladeSystem c-Class infrastructure (c3000 Enclosure or c7000 Enclosure). It is the enclosure management processor, subsystem, and firmware base that supports an HP BladeSystem c-Class enclosure and all the managed devices contained within the enclosure.

Onboard Administrator provides wizards for simple, fast setup and configuration; highly available and secure access to the HP BladeSystem infrastructure; security roles for server, network, and storage administrators; agent-less health, status, and thermal logic power/cooling information and control. The Onboard Administrator enables an administrator to configure an enclosure within a few minutes and to configure multiple enclosures simultaneously.

Onboard Administrator provides a single point from which to manage server blades or switches within the enclosure. Management tasks can be performed using the Onboard Administrator GUI, command line interface, and the enclosure’s display (HP Insight Display). The Onboard Administrator GUI can be accessed from a web browser.

This document provides details about the Onboard Administrator CLI interface. For information about accessing the Onboard Administrator CLI, see Accessing the command line interface (on page 14).

For information about the Onboard Administrator GUI and the enclosure’s HP Insight Display, see the HP BladeSystem Onboard Administrator User Guide.

CLI command categories

The command reference section of this document describes the Onboard Administrator CLI commands within the following categories, in the following order:

- General commands
- Rack commands
- User account commands
- Two-Factor Authentication commands
- Directory commands
- HP SIM commands
- General management commands
- Enclosure Bay IP Addressing commands
- Enclosure network configuration commands
- Enclosure management commands
- Enclosure firmware management commands
- Blade management commands
• Interconnect management commands
• Active Health System commands
• Enclosure DVD commands
• Remote syslog commands
• USB support commands
• VLAN commands
• HP Insight Remote Support commands
• Enclosure Dynamic Power Cap commands

What's new

The following commands were added or updated with the Onboard Administrator firmware version 4.50 release:
• SET FACTORY
• SET SERVER BOOT
• SET SERVER BOOT FIRST
• SET SERVER BOOT ONCE
Accessing the command line interface

Remote access to the Onboard Administrator

The Onboard Administrator CLI can be accessed remotely through any Telnet or SSH session.

**Telnet session**
1. Open a command-line window from a network-connected client.
2. At the prompt, telnet to the IP address of the Onboard Administrator and press Enter.
   For example, `telnet 192.168.100.130`, where the IP address is the address of your Onboard Administrator.
3. Enter a valid user name and press Enter.
4. Enter a valid password and press Enter. The CLI command prompt displays.
5. Enter commands for the Onboard Administrator.
6. To terminate the remote access telnet session, enter Exit, Logout, or Quit at the CLI command prompt.

**SSH session**
1. Start a SSH session to the Onboard Administrator using any SSH client application.
2. When prompted, enter the assigned IP address or DNS name of the Onboard Administrator and press Enter.
3. Enter a valid user name and press Enter.
4. Enter a valid password and press Enter. The CLI command prompt displays.
5. Enter commands for the Onboard Administrator.
6. To terminate the remote access SSH session, close the communication software or enter Exit, Logout, or Quit at the CLI command prompt.

Local access to the Onboard Administrator

The Onboard Administrator can be accessed locally through a serial port connector on the rear of the Onboard Administrator module. Use a laptop or another computer as a serial console to communicate with the Onboard Administrator. A laptop or PC connected to the Onboard Administrator serial port requires a null-modem cable. The minimum connection to an external console is pins 2, 3, and 5.

1. Connect a serial cable between the serial port on the computer and the corresponding serial port on the Onboard Administrator module. The following table is for the DB9 serial (RS232) port and shows the pinout and signals for the RS232 connector. The signal direction is DTE (computer) relative to the DCE (modem).

<table>
<thead>
<tr>
<th>Pin</th>
<th>Name</th>
<th>Signal direction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CD</td>
<td>&lt;&lt;&lt;</td>
<td>Carrier detect</td>
</tr>
<tr>
<td>2</td>
<td>RXD</td>
<td>&lt;&lt;&lt;</td>
<td>Receive data</td>
</tr>
<tr>
<td>3</td>
<td>TXD</td>
<td>-&gt;&gt;</td>
<td>Transmit data</td>
</tr>
</tbody>
</table>
Pin | Name | Signal direction | Description
--- | --- | --- | ---
4 | DTR | --> | Data terminal ready
5 | GND | | System ground
6 | DSR | <-- | Data set ready
7 | RTS | --> | Request to send
8 | CTS | <-- | Clear to send
9 | RI | <-- | Ring indicator

2. Use any standard communication software to launch a terminal emulation session with the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmission rate</td>
<td>9600 bps</td>
</tr>
<tr>
<td>Data bits</td>
<td>8</td>
</tr>
<tr>
<td>Parity</td>
<td>None</td>
</tr>
<tr>
<td>Stop bits</td>
<td>1</td>
</tr>
<tr>
<td>Protocol</td>
<td>None</td>
</tr>
</tbody>
</table>

3. When prompted, enter a valid user name, and then press Enter.
4. Enter a valid password, and press Enter. The CLI command prompt appears.
5. Enter commands for the Onboard Administrator.
6. To terminate the terminal session, enter Exit at the prompt.
Command line

Command line overview

The CLI can be used as an alternative method for managing the Onboard Administrator. Using the CLI can be useful in the following scenarios:

- HP Management Applications (for example: Systems Insight Manager, Insight Control tools, and so on) can query the Onboard Administrator for information these tools need to present a complete management view of HP BladeSystem enclosures and the devices contained within. This interface is also used by the Management tools to execute provisioning and configuration tasks to devices within the enclosure.

- Users can develop tools that utilize Onboard Administrator functions for data collection and for executing provisioning and configuration tasks.

- When no browser is available or you prefer to use a Linux command line interface to access management data and perform configuration tasks.

Command line conventions

CLI input is case-insensitive except when otherwise noted. Commands are organized into a tree, with approximately 30 base commands. Each of these commands can have any number of subcommands. Subcommands can also have further subcommands.

Each command used in this guide follows the conventions listed in the following table.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;lower case&gt;</td>
<td>Denotes the variable within the symbols that must be substituted with a value, such as a user name. Symbols must be removed.</td>
</tr>
<tr>
<td>UPPER CASE</td>
<td>Denotes input to be entered as shown. Unless noted, symbols are not case-sensitive.</td>
</tr>
<tr>
<td></td>
<td>Used to separate input options.</td>
</tr>
<tr>
<td>{ }</td>
<td>Denotes a list of mandatory choices that must be made. For example, SET ENCLOSURE UID {ON</td>
</tr>
<tr>
<td></td>
<td>• SET ENCLOSURE UID ON</td>
</tr>
<tr>
<td></td>
<td>• SET ENCLOSURE UID OFF</td>
</tr>
<tr>
<td>[ ]</td>
<td>Denotes an optional argument or set of characters.</td>
</tr>
<tr>
<td>&quot; &quot;</td>
<td>Used to enclose command arguments that contain spaces and special characters.</td>
</tr>
</tbody>
</table>

Reserved words

The following words can only be used in specific situations with the Onboard Administrator CLI:

- PASSWORD
Because these words indicate specific functions within the Onboard Administrator firmware, they are only allowed where explicitly defined in the help documentation for a command. Attempts to use reserved words in a command where not allowed results in an Invalid Arguments error.

A local user account cannot be created by using these reserved words.

**HP Integrity server blade restrictions**

HP Integrity server blades do not support all commands. See specific commands for restrictions on HP Integrity server blades.

The following commands are not applicable to HP Integrity server blades:
- Hponcfg
- Set Server Boot
- Set Server Boot Once
- Show Server Boot
- Show Syslog Server
- Update iLO

**Access level and privileges**

Onboard Administrator accounts are created with a username, password, privilege level, and permissions to Device bays and Interconnect bays on the Onboard Administrator. You cannot delete or modify the privileges of the default Administrator account on the Onboard Administrator. You can only change the password for the Administrator account. The following table indicates the capabilities of the user based on their privileges and permitted bays.

<table>
<thead>
<tr>
<th>Account classification</th>
<th>Capabilities</th>
<th>Account name / Privilege level</th>
<th>Bays selected for this account</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>• All commands</td>
<td>Administrator / administrator</td>
<td>All</td>
</tr>
<tr>
<td></td>
<td>• Local account, not LDAP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Only account remaining after a reset Onboard Administrator to factory defaults (account retains configured Administrator password)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Administrator account password can be reset to factory default through the Onboard Administrator serial port using L: lost</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account classification</td>
<td>Capabilities</td>
<td>Account name / Privilege level</td>
<td>Bays selected for this account</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------</td>
<td>-------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td></td>
<td>password recovery option</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Can download, add, and clear SSHKey. This key only works with the Administrator account.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OA administrator</td>
<td>• All commands</td>
<td>username / administrator</td>
<td>OA bays (all bays automatically selected)</td>
</tr>
<tr>
<td></td>
<td>• Allows access to all aspects of the HP BladeSystem Enclosure and Onboard Administrator including configuration, firmware updates, user management, and resetting default settings.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>administrator</td>
<td>• Can perform all operations to permitted device bays and interconnect bays including virtual power and console access</td>
<td>username / administrator</td>
<td>No OA bays and only selected device bays and interconnect bays</td>
</tr>
<tr>
<td></td>
<td>• administrator permission on device iLO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OA operator</td>
<td>• Allows access to all aspects of the HP BladeSystem Enclosure and Onboard Administrator, with the exception of user management</td>
<td>username / operator</td>
<td>OA bays and can have other bays selected, but the capabilities for the other bays are defined in operator*</td>
</tr>
<tr>
<td></td>
<td>• Can perform all operations to permitted device bays and interconnect bays including virtual power and console access</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• operator permission on device iLO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>operator</td>
<td>• Can perform all operations to permitted device bays and interconnect bays including virtual power and console access</td>
<td>username / operator</td>
<td>Selected device bays and interconnect bays</td>
</tr>
<tr>
<td></td>
<td>• operator permission on device iLO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OA user</td>
<td>• Can view status and</td>
<td>username / user</td>
<td>OA bays and can have other</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account classification</td>
<td>Capabilities</td>
<td>Account name / Privilege level</td>
<td>Bays selected for this account</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>user</td>
<td>• Can view status and information of selected bays</td>
<td>username / user</td>
<td>No OA bays and some device bays and interconnect bays</td>
</tr>
<tr>
<td></td>
<td>• Can view CLI history</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Can view CLI history</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Can set CLI history</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Can show CLI commands</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>information of enclosure</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Can view CLI history</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Can set password for own account</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Can set user contact information for own account</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Can show CLI commands</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*EBIPA and VLAN features allow access to all bays for an OA operator.*

**Account authentication**

**Local users**
- This is the default setting. Local user accounts are directly authenticated against a password for each account stored on the active Onboard Administrator.
- Account modifications are automatically synchronized between both Onboard Administrator modules if two are present.
- Local users may be disabled if LDAP is enabled, leaving the Administrator account as the only local account that cannot be disabled.

**LDAP users**
- The Enable/Disable LDAP is an optional setting. LDAP enabled can be used with local users enabled or disabled.
- The Onboard Administrator will use configured LDAP server and search context to request account authentication.
- Configuration of the LDAP group will determine the privileges instead of the username.
- If a user is configured for multiple groups with different privileges and bay permissions, then the user will have the highest privileges and the combination of all permitted bays.
- In version 2.10 or higher, if the user logged into the Onboard Administrator is an LDAP user then the Onboard Administrator enforces the iLO license and requires that the iLO have a Select license before allowing the AutoLogin to iLO.

**AutoLogin to iLO**

The following table indicates Onboard Administrator account privileges mapped to iLO privileges when using Onboard Administrator AutoLogin.
<table>
<thead>
<tr>
<th>iLO privileges</th>
<th>administrator</th>
<th>operator</th>
<th>user</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administer user accounts</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote console access</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Virtual power and reset</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Virtual media</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Configure iLO settings</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Login to iLO</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
**General commands**

**CLEAR SCREEN**

- **Command:**
  
  CLEAR SCREEN

- **Description:**
  
  Clears the terminal screen

- **Access level:**
  
  Administrator, Operator, User

**EXIT**

- **Command:**
  
  EXIT

- **Description:**
  
  Exits the command line interpreter

- **Access level:**
  
  Administrator, Operator, User

**HELP**

- **Command:**
  
  HELP <command>

- **Description:**
  
  If you supply a command, the usage and help text for the command appears. If no argument is given, all base commands appear.

- **Access level:**
  
  Administrator, Operator, User

- **Example:**
  
  OA-0018FE27577F> HELP
  
  ADD | ASSIGN | CLEAR | CONNECT | DISABLE | DISCOVER | DOWNLOAD | EDIT | ENABLE | EXIT | FORCE | GENERATE | HELP | HISTORY | HPONCFG | LOGOUT | PING | POWEROFF | POWERON | QUIT | REBOOT | REMOVE | RESET | RESTART | SAVE | SEND | SET | SHOW | SLEEP | TEST | UNASSIGN | UPDATE | UPLOAD

**LOGOUT**

- **Command:**
LOGOUT

- **Description:**
  Exits the command line interpreter

- **Access level:**
  Administrator, Operator, User

QUIT

- **Command:**
  QUIT

- **Description:**
  Exits the command line interpreter

- **Access level:**
  Administrator, Operator, User
Rack commands

SET RACK NAME

- **Command:**
  
  SET RACK NAME <rack name>

- **Description:**
  
  Sets the rack name

- **Access level/Bay level:**
  
  OA administrator, OA operator

- **Restrictions:**
  
  The <rack name> must be a maximum of 32 characters long and includes all alphanumeric, the dash, and the underscore characters.
  
  UnnamedRack is the default rack name.

SHOW RACK INFO

- **Command:**
  
  SHOW RACK INFO

- **Description:**
  
  Displays the rack information for the enclosure

- **Access level/Bay level:**
  
  All

- **Restrictions:**
  
  None

- **Example:**

  OA-0018FE27577F> SHOW RACK INFO
  
  Rack Information:

  Product Description: ASSY, RACK 10642 G2
  Part Number: 383573-001
  Rack Identifier: 2UJ848000H
  Rack U Height: 42

  Or

  Location hardware not found (No hardware support)
  Or

  Location data error (Hardware support available – invalid data)
SHOW RACK NAME

- **Command:**
  
  SHOW RACK NAME

- **Description:**
  
  Displays the user defined rack name setting for the enclosure

- **Access level/Bay level:**
  
  All

- **Restrictions:**
  
  None

- **Example:**
  
  OA-0018FE27577F> SHOW RACK NAME
  
  Rack Name: UnnamedRack

SHOW TOPOLOGY

- **Command:**
  
  SHOW TOPOLOGY [IPV6]

- **Description:**
  
  o Displays information about the enclosures connected by the enclosure link.
  
  o Displays a table with the enclosure name, UUID, Enclosure Rack U Position, overall health of the enclosure, and the IP address.
  
  o Displays IPv4 information by default. To display IPv6 information, enter the IPV6 keyword

- **Access level/Bay level:**
  
  All

- **Restrictions:**
  
  To display IPv6 address and address type only, use the IPV6 keyword.

- **Example:**
  
  OA-0018FE2F6941> show topology

  Detecting linked enclosures ..

  Rack Topology (top-down)

  Rack UUID: 09USE818AMMP
  Rack Name: r12

<table>
<thead>
<tr>
<th>Enclosure Name</th>
<th>Status</th>
<th>Local</th>
<th>IP Address</th>
<th>UUID</th>
</tr>
</thead>
<tbody>
<tr>
<td>USE82AMMP</td>
<td>OK</td>
<td>Yes</td>
<td>111.22.1.58</td>
<td>09USE82AMMP 6</td>
</tr>
<tr>
<td>USE812AMMP</td>
<td>OK</td>
<td>No</td>
<td>111.22.1.59</td>
<td>09USE812AMMP</td>
</tr>
</tbody>
</table>

--hardware not found--
USE813AMMP               OK      No      111.22.1.60     09USE813AMMP
--data error--

OA-E4115BECFBAB> SHOW TOPOLOGY IPV6

Detecting linked enclosures ....

Rack Topology (top-down)

Rack UUID: 09SGH211PHT1
Warning! Enclosures have different rack names!

<table>
<thead>
<tr>
<th>Enclosure Name</th>
<th>Rack Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>OA-E83935AC65EF</td>
<td>UnnamedRack</td>
</tr>
<tr>
<td>1234567890</td>
<td>Rack103</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Enclosure Name</th>
<th>Local</th>
<th>IP Address</th>
</tr>
</thead>
</table>
User account commands

ADD USER

- **Command:**
  
  ADD USER "<user name>" ["<password>"]

- **Description:**
  
  Adds a user to the system. If you do not provide a password, you are prompted for one. If script mode is enabled and the password is not provided, the password is assigned an unmatched string. This unmatched string requires an enclosure administrator to change the password to allow the new user to access the system.

- **Access level/Bay level:**
  
  OA administrator

- **Restrictions:**
  
  - A maximum of 30 user accounts can be configured in FIPS Mode OFF, while a maximum of 21 user accounts can be configured in FIPS Mode ON or DEBUG. The maximum user account limit includes reserved accounts such as the Administrator and Virtual Connect accounts.
  
  - The `<user name>` must begin with a letter, is case sensitive, and must be unique to all other user names and group names. The `<user name>` must be 1 to 40 characters long and can include all alphanumeric characters, the dash, and the underscore.
  
  - Reserved user names are: ALL (case insensitive), ADMINISTRATOR (case insensitive), switch1, switch2, switch3, switch4, switch5, switch6, switch7, switch8, ldapuser, nobody, tbmuser_, vcmuser_, and vcmuser.
  
  - If you do not specify `<password>`, you are prompted for a password.
    
    If `<password>` is provided in the same line as the command and contains spaces or hash characters (#), it must be enclosed in double quotes.
    
    In FIPS Mode OFF with strong passwords disabled, the password must be 3 to 40 characters in length. The default is 3. The password can include any printable character.
    
    In FIPS Mode ON/DEBUG, or FIPS Mode OFF with strong passwords enabled, the password must be 8 to 40 characters in length. The default is 8. The password must contain at least one character from three of the four types of characters: uppercase, lowercase, numeric, and non-alphanumeric.

ASSIGN

- **Command:**
  
  ASSIGN {SERVER | INTERCONNECT} {<bay number> | ALL | <bay number>-<bay number>} {"<user name>" | LDAP GROUP "<LDAP group name>"} *OR* ASSIGN OA {"<user name>" | LDAP GROUP "<LDAP group name>"}

  Assigns one or more bays to a user or group
User account commands

**ASSIGN OA**

- **Command:**
  ```
  ASSIGN OA {"<user name>" | LDAP GROUP "<LDAP group name>"}
  ```
- **Description:**
  Assigns the specified user or LDAP group access privilege to the Onboard Administrator bays.
- **Access level/Bay level:**
  OA administrator
- **Restrictions:**
  The `<user name>` is case sensitive.

**DISABLE USER**

- **Command:**
  ```
  DISABLE USER "<user name>"
  ```
- **Description:**
  Disables a user account. The system immediately logs out the user and prevents the user from logging in until the account is enabled. CLI sessions are terminated and all future SOAP web accesses fail.
- **Access level/Bay level:**
  OA administrator
- **Restrictions:**
  - The `<user name>` is case sensitive.
  - You cannot disable the built-in Administrator account

**DISABLE STRONG PASSWORDS**

- **Command:**
  ```
  DISABLE STRONG PASSWORDS
  ```
- **Description:**
  Removes strong password requirements for user passwords
- **Access level/Bay level:**
  OA administrator
- **Restrictions:**
  - Only Administrators with Onboard Administrator permission are allowed to manage strong passwords.
You cannot disable strong passwords when in FIPS Mode ON/DEBUG.

**ENABLE STRONG PASSWORDS**

- **Command:**
  
  ENABLE STRONG PASSWORDS

- **Description:**
  When enabled, this command requires that a user’s password be 8 to 40 characters in length. The password must contain at least one character from three of the four categories.
  
  The four categories include:
  
  - Uppercase
  - Lowercase
  - Numeric
  - Non-alphanumeric

- **Access level/Bay level:**
  
  OA administrator

- **Restrictions:**
  
  - Only Administrators with Onboard Administrator permission are allowed to manage strong passwords.
  
  - Strong passwords are enabled by default in FIPS Mode ON/DEBUG.

**ENABLE USER**

- **Command:**
  
  ENABLE USER "<user name>"

- **Description:**
  Enables a user account that was previously disabled by the DISABLE USER command

- **Access level/Bay level:**
  
  OA administrator

- **Restrictions:**
  
  The <user name> is case sensitive.

**HISTORY**

- **Command:**
  
  HISTORY

- **Description:**
  Shows the history of commands for the current session

- **Access level/Bay level:**
  
  All
• **Restrictions:**
  None

## REMOVE USER

- **Command:**
  REMOVE USER {ALL | "<user name>" | CERTIFICATE "<user name>"}

- **Description:**
  Removes a user from the system and/or any certificate mapped to the user. If you specify ALL, then the command is run for all users except the default system accounts.

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  - The <user name> is case sensitive.
  - You cannot remove the Administrator account.

## SET MINIMUM PASSWORD LENGTH

- **Command:**
  SET MINIMUM PASSWORD LENGTH <length>

- **Description:**
  Sets a minimum length for passwords. When set, a user’s password must contain at least the number of characters specified.

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  - In FIPS Mode OFF with strong passwords disabled, the minimum password length can be from 3 to 40 characters. The default is 3.
  - In FIPS Mode ON/DEBUG, or in FIPS Mode OFF with strong passwords enabled, the minimum password length can be from 8 to 40 characters. The default is 8.

## SET PASSWORD

- **Command:**
  SET PASSWORD ["<password>"]

- **Description:**
  Sets the password of the user that executed the command. If you do not provide a password on the command line, you are prompted for one. In script mode, you must provide the password on the command line.

- **Access level/Bay level:**
  All
• **Restrictions:**
  o If `<password>` is provided in the same line as the command and contains spaces or hash characters (#), it must be enclosed in double quotes.
  o In FIPS Mode OFF with strong passwords disabled, the password must be 3 to 40 characters in length. The default is 3. The password can contain any printable character.
  o In FIPS Mode ON/DEBUG, or FIPS Mode OFF with strong passwords enabled, the password must be 8 to 40 characters in length. The default is 8. The password must contain at least one character from three of the four types of characters: uppercase, lowercase, numeric, and non-alphanumeric.

To modify the minimum password length setting, use `SET MINIMUM PASSWORD LENGTH` (on page 29). To enable strong passwords, use `ENABLE STRONG PASSWORDS` (on page 28); to disable strong passwords, use `DISABLE STRONG PASSWORDS` (on page 27).

### SET SESSION TIMEOUT

- **Command:**
  `SET SESSION TIMEOUT <timeout>`

- **Description:**
  Sets the number of minutes before inactive sessions are removed. The default setting is 1440. To disable the session timeout, set it to zero.

- **Access level/Bay level:**
  OA administrator

- **Restriction:**
  Valid session timeout values range from 10 to 1440 minutes (24 hours).

### SET USER CONTACT

- **Command:**
  `SET USER CONTACT ["<user name>"] "<contact info>"

- **Description:**
Sets the contact information field for the user. If `<user name>` is not specified, the command modifies the contact information of the user who executed the command.

- **Access level/Bay level:**
  - All users can modify their own contact information.
  - The OA administrator can modify all users.
- **Restrictions:**
  - The `<user name>` is case sensitive.
  - The `<contact info>` must be a maximum of 20 characters long and includes all alphanumeric characters, the dash, the underscore, and spaces.
  - The default contact information is blank.
  - If `<contact info>` includes spaces or hash characters (#), include it within double quotes.

### SET USER FULLNAME

- **Command:**
  ```
  SET USER FULLNAME ["<user name>"] "<full name>"
  ```
- **Description:**
  Sets a user's full name. If you do not specify `<user name>`, the command modifies the full name of the user who is currently logged in.
- **Access level/Bay level:**
  - OA administrator (can modify the full name of others).
  - All users can modify their own full name.
- **Restrictions:**
  - The `<user name>` is case sensitive.
  - The `<full name>` must be 1 to 20 characters in length. It may include any alphanumeric characters, the dash (-), underscore (_), and space characters. If the `<full name>` includes spaces or hash characters (#), include it within double quotes.
  - The default full name is blank.

### SET USER PASSWORD

- **Command:**
  ```
  SET USER PASSWORD "<user name>" ["<new password>"]
  ```
- **Description:**
  Sets a user's password. If you do not supply a password on the command line, you are prompted for one. In script mode, you must supply a password on the command line.
- **Access level/Bay level**
  - OA administrator (can modify the full name of others)
  - OA operator and user access level users can change their own passwords.
- **Restrictions:**
  - The `user name` is case sensitive.
Only OA administrators can modify another user’s password. Only the Administrator account can modify the password of the Administrator account.

The `<user name>` argument is case sensitive.

If the password is provided in the same line as the command and contains spaces or hash characters (#), it must be enclosed in double quotes.

In FIPS Mode OFF with strong passwords disabled, the password must be 3 to 40 characters in length. The default is 3. The password can contain any printable character.

In FIPS Mode ON/DEBUG, or FIPS Mode OFF with strong passwords enabled, the password must be 8 to 40 characters in length. The default is 8. The password must contain at least one character from three of the four types of characters: uppercase, lowercase, numeric, and non-alphanumeric.

To modify the minimum password length setting, use `SET MINIMUM PASSWORD LENGTH` (on page 29). To enable strong passwords, use `ENABLE STRONG PASSWORDS` (on page 28); to disable strong passwords, use `DISABLE STRONG PASSWORDS` (on page 27).

SHOW PASSWORD SETTINGS

- **Command:**
  SHOW PASSWORD SETTINGS

- **Description:**
  Displays the current minimum password length and strong password settings

- **Access level/Bay level:**
  All users

- **Restrictions:**
  None

- **Example:**
  OA-0018FE27577F>SHOW PASSWORD SETTINGS
  Strong Passwords: Disabled
  Minimum Password Length: 3

SHOW SESSION TIMEOUT

- **Command:**
  SHOW SESSION TIMEOUT

- **Description:**
  Displays the current Onboard Administrator user session timeout. The session timeout is the number of minutes before inactive sessions are removed.

- **Access level/Bay level:**
  All

- **Restriction:**
  None

- **Example:**
  >SHOW SESSION TIMEOUT
  Session Timeout: 1440 minutes
SHOW USER

- **Command:**
  
  SHOW USER [LIST | 
  "<user name>"]

- **Description:**
  
  o Displays the user's full name, contact information, access rights, account status, and bays that the user can access.
  
  o If you enter **LIST** and you are an OA administrator, the information for every user is listed. An asterisk before a user name denotes the current user.
  
  o If a user name or **LIST** is not entered, information for the current user is displayed.

- **Access level/Bay level:**
  
  All

- **Restrictions:**
  
  o The `<user name>` is case sensitive.
  
  o Users who do not have OA administrator access levels can only view their user information.

- **Example:**
  
  OA-0018FE27577F> SHOW USER
  Local User "Administrator" Information:
  
  Full name: System Administrator
  Contact Info:
  User Rights: Admin
  Account Status: Enabled
  Server Bay Access List: 1 1A 1B 2 2A 2B 3 3A 3B 4 4A 4B 5 5A 5B 6 6A 6B 7 7A 7B 8 8A 8B
  Interconnect Bay Access List: 1 2 3 4
  OA Access: Yes

SLEEP

- **Command:**
  
  SLEEP <seconds>

- **Description:**
  
  Pauses the sessions for a fixed period of time. This command is useful for adding delays to scripts. After the pause has started, you cannot continue the session before time runs out. However, you can terminate the session and start another session.

- **Access level/Bay level:**
  
  All

- **Restrictions:**
  
  The `<seconds>` field must be a whole number from 1 to 86400.

UNASSIGN

- **Command:**
UNASSIGN {SERVER | INTERCONNECT} {<bay number> | ALL | <bay number>-<bay number>} {"<user name>" | LDAP GROUP "<LDAP group name>"} *OR* UNASSIGN OA {"<user name>" | LDAP GROUP "<LDAP group name>"}

- **Description:**
  Removes a bay from the user

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  The <user name> is case sensitive.

**UNASSIGN OA**

- **Command:**
  UNASSIGN OA {"<user name>" | LDAP GROUP "<LDAP group name>"}

- **Description:**
  Removes the specified user's or group's access privileges to the Onboard Administrator bays.

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  The <user name> is case sensitive.
Two-Factor Authentication commands

ADD CA CERTIFICATE

- **Command:**
  
  ```
  ADD CA CERTIFICATE <end marker> \n  <certificate> \n  <end marker>
  ```

- **Description:**
  Adds a CA certificate on the command line. To add the certificate:
  a. Start with a string that does not appear within the certificate (the end marker).
  b. Insert a newline character by pressing Enter.
  c. Paste the certificate on the command line.
  d. Insert a newline character by pressing Enter.
  e. Insert the end marker.
  f. Issue the command by pressing Enter.

Failure to give a proper end marker before and after the certificate might cause the interface to wait for the appropriate end marker indefinitely.

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  - This command is only available in script mode.
  - The maximum length of the certificate is 8192 characters.
  - When the Onboard Administrator is operating in FIPS Mode, certificates must have a minimum RSA key length of 2048 bits, and the signature hash algorithm must be SHA1, SHA-224, SHA-256, SHA-384, or SHA-512.

DISABLE CRL

- **Command:**
  ```
  DISABLE CRL
  ```

- **Description:**
  Disables certificate revocation checks

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  None
DISABLE TWOFACTOR

- **Command:**
  DISABLE TWOFACTOR

- **Description:**
  Disables Two-Factor Authentication

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  None

DOWNLOAD CA CERTIFICATE

- **Command:**
  DOWNLOAD CA CERTIFICATE "<url>"

- **Description:**
  - Downloads a CA certificate to act as the trusted certification authority to validate user certificates when using Two-Factor Authentication.
  - Specify a URL where this certificate can be found.
  - Supported protocols are HTTP, FTP, and TFTP.
  - Format the URL as protocol://host/path/file.
  - If your FTP server does not support anonymous connections, you can specify a user name and password in the format ftp://username:password@host/path/file.
  - The URL syntax for IPv4 addresses is protocol://<ipv4 address>/path/file.
  - The URL syntax for IPv6 addresses is protocol://[<ipv6 address>]path/file.

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  - Allows the download of up to five different certificates.
  - The maximum length of the certificate is 8192 characters.
  - When the Onboard Administrator is operating in FIPS Mode, certificates must have a minimum RSA key length of 2048 bits, and the signature hash algorithm must be SHA1, SHA-224, SHA-256, SHA-384, or SHA-512.

DOWNLOAD USER CERTIFICATE

- **Command:**
  DOWNLOAD USER CERTIFICATE "<user name>" <url>

- **Description:**
  - Downloads an x.509 certificate for the user from <url>. The file at <url> must be a Base64 PEM encoded file.
• Downloads a CA certificate used in Two-Factor Authentication.

**Access level/Bay level:**
OA administrator

**Restrictions:**
- The maximum length of the certificate is 8192 characters.
- When the Onboard Administrator is operating in FIPS Mode, certificates must have a minimum RSA key length of 2048 bits, and the signature hash algorithm must be SHA1, SHA-224, SHA-256, SHA-384, or SHA-512.

### REMOVE CA CERTIFICATE

- **Command:**
  REMOVE CA CERTIFICATE "<certificate name>"

- **Description:**
  Removes the trust certificate corresponding to the SHA1 <certificate name>. Any users having their certificates issued by this CA can no longer login if Two-Factor Authentication is enabled.

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  None

### REMOVE USER CERTIFICATE

- **Command:**
  REMOVE USER CERTIFICATE "<user name>"

- **Description:**
  Removes the user certificate. If Two-Factor Authentication is enabled, this user no longer has access through HTTPS.

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  None

### SET USER CERTIFICATE

- **Command:**
  SET USER CERTIFICATE "<user name>" <end marker> <\n> <certificate> <\n> <end marker>

- **Description:**
  Maps a certificate (for certificate-based authentication) to the specified Onboard Administrator user account. To add the certificate:
a. Start with a string that does not appear within the certificate (the end marker).
b. Insert a newline character by pressing Enter.
c. Paste the certificate on the command line.
d. Insert a newline character by pressing Enter.
e. Insert the end marker.
f. Issue the command by pressing Enter.

Failure to give a proper end marker before and after the certificate might cause the interface to wait for the appropriate end marker indefinitely.

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  - This command is only available in script mode.
  - The maximum length of the certificate is 8192 characters.
  - When the Onboard Administrator is operating in FIPS Mode, certificates must have a minimum RSA key length of 2048 bits, and the signature hash algorithm must be SHA1, SHA-224, SHA-256, SHA-384, or SHA-512.

**SHOW CA CERTIFICATES**

- **Command:**
  SHOW CA CERTIFICATES

- **Description:**
  Displays a list of installed CA certificates

- **Access level/Bay level:**
  OA Administrator

- **Restrictions:**
  None

- **Example:**
  OA-0016355E560A> SHOW CA CERTIFICATE
  Details for ca certificate 1
  certificateVersion = 3
  issuerOrganization = ca.com
  issuerOrganizationalUnit = IT Infrastructure
  issuerCommonName = Hewlett-Packard Primary Class 2 Certification Authority
  subjectOrganization = hp.com
  subjectOrganizationalUnit = IT Infrastructure
  subjectCommonName = Hewlett-Packard Primary Class 2 Certification Authority
  validFrom = 1997-12-30T00:00:00Z
  validTo = 2012-12-29T23:59:59Z
  extensionCount = 7
SHOW TWOFACTOR INFO

- **Command:**
  SHOW TWOFACTOR INFO

- **Description:**
  Displays the configuration details for Two-Factor Authentication

- **Access level/Bay level:**
  All

- **Restrictions:**
  None

- **Example:**
  OA-0018FE27577F> SHOW TWOFACTOR INFO
  Two Factor Authentication:
  Enabled : Disabled
  Certificate Revocation : Disabled
  Certificate Owner Field : Subject

```bash
```
Directory commands

ADD LDAP CERTIFICATE

- **Command:**
  
  ADD LDAP CERTIFICATE <end marker> \n  <certificate> \n  <end marker>

- **Description:**
  
  Adds an LDAP certificate on the command line. To add the certificate:
  
  a. Start with a string that does not appear within the certificate (the end marker).
  b. Insert a newline character by pressing Enter.
  c. Paste the certificate on the command line.
  d. Insert a newline character by pressing Enter.
  e. Insert the end marker.
  f. Issue the command by pressing Enter.

  Failure to give a proper end marker before and after the certificate might cause the interface to wait for the appropriate end marker indefinitely.

- **Access level/Bay level:**
  
  OA administrator

- **Restrictions:**
  
  o The maximum length of the certificate is 8192 characters.
  o When the Onboard Administrator is operating in FIPS Mode, certificates must have a minimum RSA key length of 2048 bits, and the signature hash algorithm must be SHA1, SHA-224, SHA-256, SHA-384, or SHA-512.
  o This command is only available in script mode.

ADD LDAP GROUP

- **Command:**
  
  ADD LDAP GROUP "<group name>"

- **Description:**
  
  Adds an LDAP group to the group. This group must match a group in the directory server.

- **Access level/Bay level:**
  
  OA administrator

- **Restrictions:**
  
  o The maximum number of LDAP groups is 30.
  o Group name must be 1 to 255 characters in length.
  o Character set includes all printable characters, except quotation marks and new lines.
The group name must start with an alpha character.

ASSIGN for LDAP

- **Command:**
  ASSIGN {SERVER | INTERCONNECT} {<bay number> | ALL | <bay number>-<bay number>} {"<user name>" | LDAP GROUP "<LDAP group name>"} *OR* ASSIGN OA {"<user name>" | LDAP GROUP "<LDAP group name>"}

- **Description:**
  Assigns the bay to a specified LDAP group, providing access to the bay at the access level of the group

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  None

ASSIGN OA LDAP GROUP

- **Command:**
  ASSIGN OA {"<user name>" | LDAP GROUP "<LDAP group name>"}

- **Description:**
  Assigns access to the Onboard Administrator to the specified group

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  None

DISABLE LDAP

**NOTE:** If LDAP is enabled, local accounts are disabled, and the LDAP server becomes unavailable, you can recover by booting into Lost Password mode. When booting in Lost Password mode, the local Administrator password will be reset, LDAP is disabled, and Local Logins are re-enabled

- **Command:**
  DISABLE LDAP

- **Description:**
  Disables directory authentication

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  None
DOWNLOAD LDAP CERTIFICATE

- **Command:**
  DOWNLOAD LDAP CERTIFICATE "<url>

- **Description:**
  - Downloads an LDAP certificate to establish a trusted relationship with the LDAP server.
  - The `<url>` specifies the location of the certificate to be downloaded.
  - Supported protocols are HTTP, FTP, and TFTP.
  - Format the URL as protocol://host/path/file.
  - The URL syntax for IPv4 addresses is protocol://<ipv4 address>/path/file.
  - The URL syntax for IPv6 addresses is protocol://[<ipv6 address>]/path/file.
  - If your FTP server does not support anonymous connections, then you can specify a user name and password in the format ftp://username:password@host/path/file.

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  - The maximum length of the certificate is 8192 characters.
  - When the Onboard Administrator is operating in FIPS Mode, certificates must have a minimum RSA key length of 2048 bits, and the signature hash algorithm must be SHA1, SHA-224, SHA-256, SHA-384, or SHA-512.

ENABLE LDAP

**NOTE:** If LDAP is enabled, local accounts are disabled, and the LDAP server becomes unavailable, you can recover by booting into Lost Password mode. When booting in Lost Password mode, the local Administrator password will be reset, LDAP is disabled, and Local Logins are re-enabled.

- **Command:**
  ENABLE LDAP [NOLOCAL]

- **Description:**
  Enables directory authentication. If you use the NOLOCAL option, local users are not enabled.

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  Before you can enable LDAP, configuration must be complete.

REMOVE LDAP CERTIFICATE

- **Command:**
  REMOVE LDAP CERTIFICATE "<certificate name>"
• **Description:**
  o Removes the trust certificate corresponding to the MD5 `<certificate name>`.
  o This command revokes trust in the LDAP server associated with the certificate.

• **Access level/Bay level:**
  OA administrator

• **Restrictions:**
  None

**REMOVE LDAP GROUP**

• **Command:**
  REMOVE LDAP GROUP {ALL | `<group name>`}

• **Description:**
  Removes the LDAP group from the system. If you specify ALL, then all LDAP groups are removed from the system.

• **Access level/Bay level:**
  OA administrator

• **Restrictions:**
  Before you can enable the LDAP group, configuration must be complete.

**SET LDAP GROUP ACCESS**

• **Command**
  SET LDAP GROUP ACCESS `<group name>` {ADMINISTRATOR | OPERATOR | USER}

• **Description:**
  o Sets the LDAP group access level.
  o Additionally, use the ASSIGN OA command to give a user or group rights to the Onboard Administrator.

• **Access level/Bay level:**
  OA administrator

• **Restrictions:**
  None

**SET LDAP GROUP DESCRIPTION**

• **Command:**
  SET LDAP GROUP DESCRIPTION `<group name>` `<description>`

• **Description:**
  Sets the LDAP group description field

• **Access level/Bay level:**
OA administrator

- **Restrictions:**
  - Must be 0 to 58 characters in length.
  - Valid characters are all alphanumeric, the underscore (_), the dash (-), and spaces.
  - If the group name or description field contains spaces or zero characters, use double quotes.

### SET LDAP NAME MAP

- **Command:**
  
  `SET LDAP NAME MAP {ON|OFF}`

- **Description:**
  
  Turns on NT name mapping to enable the user to enter their NT domain\username

- **Access level/Bay level:**
  
  OA administrator

- **Restrictions:**
  
  None

### SET LDAP GCPORT

- **Command:**
  
  `SET LDAP GCPORT { <port number> | NONE }`

- **Description:**
  
  Sets the TCP port number of the LDAP Global Catalog SSL service. Port 3269 is the standard value.

- **Access level/Bay level:**
  
  OA administrator

- **Restrictions:**
  
  The valid port number range is 1 to 65535.

### SET LDAP PORT

- **Command:**
  
  `SET LDAP PORT { <port number> | NONE }`

- **Description:**
  
  Sets the TCP port number of the LDAP SSL service. Port 636 is the standard value.

- **Access level/Bay level:**
  
  OA administrator

- **Restrictions:**
  
  The valid port number range is 1 to 65535
SET LDAP SEARCH

- **Command:**
  
  SET LDAP SEARCH {1-6} "<search content>"

- **Description:**
  
  Sets up to six search contexts in priority order

- **Access level/Bay level:**
  
  OA administrator

- **Restrictions:**
  
  None

SET LDAP SERVER

- **Command:**
  
  SET LDAP SERVER {<ip address> | <dns name> | NONE }

- **Description:**
  
  - Sets the IP address or the DNS name of the LDAP server used for authentication.
  - To set the LDAP server field to blank, use keyword NONE.

- **Access level/Bay level:**
  
  OA administrator

- **Restrictions:**
  
  - `<ip address>` can be either an IPv4 address or an IPv6 address. IPv6 addresses must be informed without the network prefix length.
  - IPv4 address—###.###.###.### where ### ranges from 0 to 255
  - IPv6 address—####:####:####:####:####:####:####:#### where #### ranges from 0 to FFFF. A compressed version of the same IPv6 address is also supported.

SHOW LDAP CERTIFICATE

- **Command:**
  
  SHOW LDAP CERTIFICATE

- **Description:**
  
  Displays all LDAP certificates that are in effect on the Onboard Administrator

- **Access level/Bay level:**
  
  OA administrator

- **Restrictions:**
  
  None

- **Example:**
  
  OA-0016355E560A> SHOW LDAP CERTIFICATE
  1 Certificate name: 17D6A5ECBF51A1A47D44C1CDD29D19EE.pem
  -----BEGIN CERTIFICATE-----
SHOW LDAP GROUP

- **Command:**
  
  SHOW LDAP GROUP {LIST | "<group name>")

- **Description:**
  
  This command displays the LDAP group information. If you specify LIST, then a list of all the LDAP groups appears.

- **Access level/Bay level:**
  
  OA administrator, OA operator, OA user

- **Restrictions:**
  
  None

- **Example:**
  
  OA-0018FE27577F> SHOW LDAP GROUP LIST
  
  Privilege   LDAP Group / Level Description
  Operator     Widget.OPS.Team@hp.com

SHOW LDAP INFO

- **Command:**
  
  SHOW LDAP INFO

- **Description:**
  
  Displays the LDAP settings, including enabled or disabled status, LDAP server, LDAP port, search contexts, and NT mapping state

- **Access level/Bay level:**
  
  All

- **Restrictions:**
  
  None

- **Example:**
  
  OA-0018FE27577F> show ldap info
  
  Directory Services (LDAP)
  
  Enabled : Disabled
  Local Users Enabled : Enabled
  NT Name Mapping : Disabled
  Directory Server : 

Directory commands  46
TEST LDAP

- **Command:**
  
  TEST LDAP "<username>" "<password>"

- **Description:**
  Run LDAP tests and optionally attempt to log in to the LDAP server using the user name and password.

- **Access level/Bay level:**
  
  OA administrator

- **Restrictions:**
  
  - The user name can be 0 to 256 characters in length. Use a double backslash for the user name (for example, "domain-name\user-name").
  - The password can be 0 to 1024 characters in length.

UNASSIGN for LDAP

- **Command:**
  
  UNASSIGN {SERVER | INTERCONNECT} {<bay number> | ALL | <bay number>-<bay number>} {"<user name>" | LDAP GROUP "<LDAP group name>"} *OR* UNASSIGN OA {"<user name>" | LDAP GROUP "<LDAP group name>"}

- **Description:**
  
  Disables access to the bays for the group specified

- **Access level/Bay level:**
  
  OA administrator

- **Restrictions:**
  
  None

UNASSIGN OA LDAP GROUP

- **Command:**
  
  UNASSIGN OA {"<user name>" | LDAP GROUP "<LDAP group name>"}

- **Description:**
  
  Disables access to the Onboard Administrator for the group specified

- **Access level/Bay level:**
  
  OA administrator

- **Restrictions:**
  
  None
None
HP SIM commands

ADD HPSIM CERTIFICATE

- **Command:**
  
  ```
  ADD HPSIM CERTIFICATE <end marker> <\n> <certificate> <\n> <end marker>
  ```

- **Description:**
  Adds an HP SIM certificate on the command line. To add the certificate:
  a. Start with a string that does not appear within the certificate (the end marker).
  b. Insert a newline character by pressing Enter.
  c. Paste the certificate on the command line.
  d. Insert a newline character by pressing Enter.
  e. Insert the end marker.
  f. Issue the command by pressing Enter.

  Failure to give a proper end marker before and after the certificate might cause the interface to wait for the appropriate end marker indefinitely.

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  o This command is only available in script mode.
  o The maximum length of the certificate is 8192 characters.
  o When the Onboard Administrator is operating in FIPS Mode, certificates must have a minimum RSA key length of 2048 bits, and the signature hash algorithm must be SHA1, SHA-224, SHA-256, SHA-384, or SHA-512.

DOWNLOAD HPSIM CERTIFICATE

- **Command:**
  
  ```
  DOWNLOAD HPSIM CERTIFICATE { <host> }
  ```

- **Description:**
  o Downloads an HP SIM certificate from the specified IP address or fully-qualified DNS system name (for example, nwest-office.acme.com).
  o The `<host>` value can be an IPv4 address, an IPv6 address, or a DNS name.
  o For IPv4, specify the address in the form `###.###.###.###`, where each `###` ranges from 0 to 255.
  o For IPv6, specify the address in the form `####:####:####:####:####:####:####:####`, where each `####` ranges from 0 to FFFF.

- **Access level/Bay level:**
OA administrator

- **Restrictions:**
  - Do not include the network prefix length with IPv6 addresses.
  - The maximum length of the certificate is 8192 characters.
  - When the Onboard Administrator is operating in FIPS Mode, certificates must have a minimum RSA key length of 2048 bits, and the signature hash algorithm must be SHA1, SHA-224, SHA-256, SHA-384, or SHA-512.
  - Onboard Administrator 4.11 and later contains HP SSO application support for determining the minimum SSO certificate requirements.

### REMOVE HP SIM CERTIFICATE

- **Command:**
  ```plaintext```
  REMOVE HP SIM CERTIFICATE "<certificate name>"
  ```plaintext```

- **Description:**
  Removes the trust certificate corresponding to the `<certificate name>`. Disables HP SIM SSO through the application (for example HP SIM) that provided the certificate without disabling other HP SIM applications.
  The `<certificate name>` can be obtained using the SHOW HP SIM INFO command.

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  None

### SET HP SIM TRUST MODE

- **Command:**
  ```plaintext```
  SET HP SIM TRUST MODE {CERTIFICATE [ON] | DISABLED [OFF]}
  ```plaintext```

- **Description:**
  Enables or disables the HP SIM SSO mode. When enabled, the trusted applications can access the Onboard Administrator GUI data without requiring additional authentication.

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  The CERTIFICATE (On) mode trusts only applications with certificates that have been uploaded to the Onboard Administrator.

### SHOW HP SIM INFO

- **Command:**
  ```plaintext```
  SHOW HP SIM INFO
  ```plaintext```
• **Description:**
  Displays the current HP SIM SSO configuration for the Onboard Administrator.
  The data includes the current HP SIM SSO Trust Mode (see `SET HPSIM TRUST MODE`) and a list of
  names that the Onboard Administrator is configured to trust using a trust certificate.

• **Access level/Bay level:**
  OA administrator

• **Restrictions:**
  None

• **Example:**
  OA-0018FE27577F> SHOW HPSIM INFO
  HPSIM Trust Mode: Disabled
  Trusted Server Certificates
  No certificates were found.
General management commands

DISABLE URB

- **Command:**
  `DISABLE URB`

- **Description:**
  Disables URB reporting.

- **Access level/Bay level:**
  OA Administrator, OA Operator

- **Restrictions:**
  None

- **Example:**
  `OA-0018FE27577F> disable urb`
  Utility Ready Blade (URB) reporting has been disabled.

DOWNLOAD OA CERTIFICATE

- **Command:**
  `DOWNLOAD OA CERTIFICATE [bay number] | ACTIVE | STANDBY] <url>`

- **Description:**
  - Downloads a CA supplied pkcs#7 file to replace the current security certificate on the system.
  - If you do not specify the Onboard Administrator (bay number>, ACTIVE, or STANDBY), the certificate is downloaded to the current (local) Onboard Administrator.
  - Specify a URL where this certificate can be found.
  - Supported protocols are HTTP, FTP, and TFTP.
  - Format the URL as protocol://host/path/file.
  - The URL syntax for IPv4 addresses is protocol://<ipv4 address>/path/file.
  - The URL syntax for IPv6 addresses is protocol://[<ipv6 address>]/path/file.
  - If your FTP server does not support anonymous connections, you can specify a user name and password in the format ftp://username:password@host/path/file.

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  - The maximum length of the certificate is 8192 characters.
  - When the Onboard Administrator is operating in FIPS Mode, certificates must have a minimum RSA key length of 2048 bits, and the signature hash algorithm must be SHA1, SHA-224, SHA-256, SHA-384, or SHA-512.
**ENABLE URB**

- **Command:**
  
  `ENABLE URB { HTTP | SMTP | BOTH }`

- **Description:**

  Enables URB reporting. URB messages may be reported using HTTP(S), SMTP, or both.

- **Access level/Bay level:**

  OA Administrator, OA Operator

- **Restrictions:**

  - For HTTP(S) reporting, an endpoint URL must be configured (use `SET URB` on page 58).
  - For SMTP reporting, an SMTP server and email address (mailbox) must be configured (use `SET URB` on page 58).

- **Example:**

  `OA-0018FE275723> enable urb smtp`
  
  Utility Ready Blade (URB) reporting via SMTP has been enabled.

**FORCE TAKEOVER**

- **Command:**

  `FORCE TAKEOVER`

- **Description:**

  Forces the redundant Onboard Administrator to become the active Onboard Administrator. The active becomes the standby and the standby becomes the active.

- **Access level/Bay level:**

  OA administrator

- **Restrictions:**

  None

**GENERATE CERTIFICATE**

- **Command:**

  `GENERATE CERTIFICATE [REQUEST | SELFSIGNED]`

- **Description:**

  - Generates a pkcs#10 certificate request or a self-signed certificate. You are prompted for the following fields to generate a certificate:

    — OA Host Name (CN)
    — Organization Name (O)
    — City or Locality (L)
    — State or Province (ST)
    — Country (C)
The Alternative Name field is used to create the X509v3 Subject Alternative Name extension attribute. The field must be empty or contain a list of keyword:value pairs separated by commas. The valid keyword:value entries include IP: <ip address> and DNS: <domain name>.

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  This command is not valid in script mode.

### GENERATE CERTIFICATE prompts

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Description</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>OA Host Name (CN)</td>
<td>This is the most important field. This is the Onboard Administrator name that appears in the browser web address field. This certificate attribute is generally referred to as the common name.</td>
<td>Must be 1 to 60 characters long. To prevent security alerts, the value of this field must match the host name exactly as it is known by the web browser. The browser compares the host name in the resolved web address to the name that appears in the certificate. For example, if the web address in the address field is <a href="https://oa-001635.xyz.com">https://oa-001635.xyz.com</a>, then the value must be oa-001635.xyz.com.</td>
</tr>
<tr>
<td>Organization Name (O)</td>
<td>The company or organization that owns this Onboard Administrator. When this information is used to generate a certificate signing request, the issuing certificate authority can verify that the organization requesting the certificate is legally entitled to claim ownership of the given company name or organization name.</td>
<td>Must be 1 to 60 characters long.</td>
</tr>
<tr>
<td>City or Locality (L)</td>
<td>The city or locality where the Onboard Administrator is located.</td>
<td>Must be 1 to 50 characters long.</td>
</tr>
<tr>
<td>State or Province (ST)</td>
<td>The state or province where the Onboard Administrator is located.</td>
<td>Must be 1 to 30 characters long.</td>
</tr>
<tr>
<td>Prompt</td>
<td>Description</td>
<td>Restrictions</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>Country (C)</td>
<td>The two-character country code that identifies the country where the Onboard Administrator is located.</td>
<td>Must be a two-character country code.</td>
</tr>
<tr>
<td>Organizational Unit</td>
<td>The unit within the company or organization that owns the Onboard Administrator.</td>
<td>(Optional) Must be 0 to 60 characters long.</td>
</tr>
<tr>
<td>Contact Person</td>
<td>The person responsible for the Onboard Administrator.</td>
<td>(Optional) Must be 0 to 60 characters long.</td>
</tr>
<tr>
<td>Email Address</td>
<td>The email address of the contact person responsible for the Onboard Administrator.</td>
<td>(Optional) Must be 0 to 60 characters long.</td>
</tr>
<tr>
<td>Surname</td>
<td>The surname of the person responsible for the Onboard Administrator.</td>
<td>(Optional) Must be 0 to 60 characters long.</td>
</tr>
<tr>
<td>Given Name</td>
<td>The given name of the person responsible for the Onboard Administrator.</td>
<td>(Optional) Must be 0 to 60 characters long.</td>
</tr>
<tr>
<td>Alternative Name</td>
<td>An alternative name of the person responsible for the Onboard Administrator. The name is used for creating the X509v3 Subject Alternative Name extension attribute.</td>
<td>(Optional) Must be 0 to 512 characters long. The field must either be empty or contain a list of keyword:value pairs separated by commas. The valid keyword:value entries include IP:&lt;ip address&gt; and DNS:&lt;domain name&gt;.</td>
</tr>
<tr>
<td>Initials</td>
<td>The initials of the person responsible for the Onboard Administrator.</td>
<td>(Optional) Must be 0 to 20 characters long.</td>
</tr>
<tr>
<td>DN Qualifier</td>
<td>The distinguished name qualifier of the Onboard Administrator.</td>
<td>(Optional) Must be 0 to 60 characters long.</td>
</tr>
<tr>
<td>Challenge Password</td>
<td>The password to the certificate-signing request.</td>
<td>(Optional) Must be 0 to 20 characters long.</td>
</tr>
<tr>
<td>Unstructured Name</td>
<td>This is for additional information (for example, an unstructured name that is assigned to the Onboard Administrator).</td>
<td>(Optional) Must be 0 to 60 characters long.</td>
</tr>
</tbody>
</table>

**GENERATE KEY**

- **Command:**

  GENERATE KEY { ALL | SECURESH | SSL } [ 1024 | 2048 ][ HASH_ALGORITHM { SHA1 | SHA-224 | SHA-256 | SHA-384 | SHA-512 }]

- **Description:**
  - Generates new private keys associated with the Onboard Administrator SSH service or SSL web services.
  - If the optional key size is not specified, 2048 is the default.
  - If the hash algorithm is not specified, SHA-256 is the default for SSL keys.
  - Any self-signed or uploaded web service certificates generated using existing keys are reset.
- The key type is always RSA.

**Access level/Bay level:**
OA administrator

**Restrictions:**
- The SHA-224 hash algorithm may not work with some web browsers without the latest encryption libraries.
- When the Onboard Administrator is operating in FIPS Mode, certificates must have a minimum RSA key length of 2048 bits, and the signature hash algorithm must be SHA1, SHA-224, SHA-256, SHA-384, or SHA-512.

### PING

**Command:**

PING [IPv6 [INTERNAL]] [number] {ip address} | "<server name>"

**Description:**
- Sends ICMP echo messages to a remote IP device.
- If INTERNAL is specified, the command tries to reach only those hosts internal to the enclosure (iLO or interconnect management interfaces only).
- If <number> is omitted, then only four packets are sent. If <number> is zero, then the command attempts to trace the network route to the host (IPv4 only).
- Specify an IPv4 address in the form ###.##.###.###, where each ### ranges from 0 to 255.
- Specify an IPv6 address in the form ####:####:####:####:####:####:####:####, where each #### ranges from 0 to FFFF.
- Packets are sent out at one-second intervals to prevent strain on the network.

**Access level/Bay level:**
All

**Restrictions:**
- The <number> value cannot be greater than 9999 or negative. A <number> greater than 9999 results in an error or four packets being sent. A negative number results in an error.

### SET DEVICE SERIAL_NUMBER BLADE

**Command:**

SET DEVICE SERIAL_NUMBER BLADE <bay number> "<serial number>"

**Description:**
Sets the serial number of the specified Storage, Tape, or I/O expansion blade.

**Access level/Bay level:**
OA administrator

**Restrictions:**
- Length must be 10 characters. All printable characters are allowed.
- This operation cannot be performed on server blades.
SET FACTORY

- **Command:**
  
  SET FACTORY [RESTORE_FACTORY_PASSWORD]

  Restores all settings back to the factory defaults. All existing settings are lost. The Administrator’s password does not change to the factory default unless you specify `RESTORE_FACTORY_PASSWORD`. (The factory default Administrator password is indicated on the label affixed to the Onboard Administrator.)

- **Description:**
  - Restores the Onboard Administrator to its factory defaults. In addition, resets the Administrator password to its default.
  - The Onboard Administrator restarts after all changes are made.
  - All existing settings are lost when this operation is run.

  **IMPORTANT:** Before resetting factory defaults, save your configuration. To upload a script containing your current configuration, use the [UPLOAD CONFIG](on page 154) command. You can use this script later to restore settings that are lost after a factory reset.

  **NOTE:** After a factory reset, the enclosure IPv6 network settings (IPv6, SLAAC, and DHCPv6) are enabled by default.

- **Access level/Bay level:**
  - OA administrator

- **Restrictions:**
  - You cannot run `SET FACTORY` in FIPS Mode ON/DEBUG.

SET SCRIPT MODE

- **Command:**
  
  SET SCRIPT [MODE] {ON | OFF}

- **Description:**
  - When enabled, script mode prevents commands from prompting for input or confirmation. All actions are performed without confirmation. Default values are used for any parameters that normally require user intervention.
  - Some commands are available only if script mode is enabled.
  - While script mode is enabled, pagination is disabled for commands that display large amounts of data. In other words, data is displayed continuously rather than a screen at a time.
  - Script mode is disabled by default. If you enable script mode, the setting remains in effect only for the current CLI session. While script mode is enabled, the CLI prompt indicates so, as in the following example:

    OA-9C8E99224631 [SCRIPT MODE] >

- **Access level/Bay level:**
  - All

- **Restrictions:**
Script mode may change the behavior, required parameters, or output for certain CLI commands.

### SET URB

- **Command:**
  
  ```
  SET URB [ URL | INTERVAL | PROXY URL | SMTPSERVER | MAILBOX ]
  ```

- **Description:**
  
  Sets settings for URB reporting

  - **SET URB URL { <url> }**
    
    sets the URB endpoint URL.

  - **SET URB PROXY URL { <url> }**
    
    sets the proxy URL to use when sending URB messages.

  - **SET URB INTERVAL { HOURLY <minute> | DAILY <hour> | WEEKLY <day> <hour> | MONTHLY <day> <hour> }**
    
    sets the interval at which URB messages are sent.

- **Access level/Bay level:**
  
  OA Administrator, OA Operator

- **Restrictions:**
  
  - **SET URB URL { <url> }**: The URL must be either an HTTP or HTTPS URL and can be no longer than 128 characters.

  - **SET URB PROXY URL { <url> }**: The URL can be no longer than 128 characters.

  - **SET URB INTERVAL { HOURLY <minute> | DAILY <hour> | WEEKLY <day> <hour> | MONTHLY <day> <hour> }**:
    
    - The minutes parameter must be 0-59.
    - The DAILY hour parameter must be 0-23.
    - The WEEKLY day parameter must be 1-7 where 1 is Sunday and 7 is Saturday.
    - The MONTHLY day parameter must be 1-31.

### SHOW ALL

- **Command:**
  
  ```
  SHOW ALL
  ```

- **Description:**
  
  Executes all Onboard Administrator `SHOW` commands in succession. For specific command output examples, see the individual `SHOW` commands in this guide.

- **Access level/Bay level:**
  
  All

- **Restrictions:**
  
  - This command only displays the bays for which you have privileges.

  - To save the output, you must configure your Telnet software to log the session to a file or increase the history buffer size so that the output can be copied and pasted into another file.
SHOW DEVICE SERIAL_NUMBER BLADE

- **Command:**
  
  SHOW DEVICE SERIAL_NUMBER BLADE <bay number>

- **Description:**
  Shows the specified direct attached blade device serial number

- **Access level/Bay level:**
  - All
  - Bay specific

- **Restrictions:**
  Dependent on bay privileges

- **Example:**
  OA-0016355E560A> SHOW DEVICE SERIAL_NUMBER BLADE 1
  Serial Number: USM81500RP

SHOW URB

- **Command:**
  
  SHOW URB

- **Description:**
  Displays the URB reporting settings

- **Access level/Bay level:**
  OA Administrator, OA Operator

- **Restrictions:**
  None

- **Example:**
  OA-0018FE275723> show urb
  URB Reporting: Enabled
  URB Endpoint URL:
  URB Proxy URL:
  URB Interval: Daily at hour 0
  Last Attempt: None

TEST URB

- **Command:**
  
  TEST URB

- **Description:**
  Manually sends the URB message to the endpoint. This command can be useful for testing the configuration or resending a message after a failure. If the test fails, executing the TEST URB command updates the last attempt status and log a syslog message.

- **Access level/Bay level:**
OA Administrator, OA Operator

- **Restrictions:**
  Only works if URB reporting is enabled

- **Example:**
  OA-0018FE27577F> test urb

  The OA is preparing to send a Utility Ready Blade (URB) notification. Once the message has been sent, the status will be reflected in the SHOW URB command.
Enclosure Bay IP Addressing commands

ADD EBIPA

- **Command:**
  
  ADD EBIPA {SERVER | INTERCONNECT} DNS <ip address> [{ , | - } <bay number>]

- **Description:**
  Adds a DNS server IP address to the list of DNS servers for either SERVER bays or INTERCONNECT bays.

- **Access Level/Bay level:**
  Administrator, Operator

- **Restrictions:**
  - A maximum of three DNS servers can be added for EBIPA.
  - The <ip address> must be in the form ###.###.###.###, where each ### ranges from 0 to 255.

ADD EBIPAV6

- **Command:**
  
  ADD EBIPAV6 { SERVER | INTERCONNECT } DNS <ipv6 address> [ ALL | <bay number> [{ , | - } <bay number>] ]

- **Description:**
  Adds an EBIPA DNS server IPv6 address to the list of DNS servers for either server bays or interconnect bays.

- **Access Level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  - A maximum of three IPv6 DNS servers can be added for EBIPA.
  - A bay number or bay range may be specified. If no bay number or bay range is specified, the IPv6 DNS server is added to all servers or interconnects.
  - The <ip address> must be in the form ####:####:####:####:####:####:####:####/###, where #### ranges from 0 to FFFF. A compressed version of the same IPv6 address is also supported.

DISABLE EBIPA
**CAUTION:** This command causes the affected devices to lose their current EBIPA-configured address. Any clients accessing the devices via that address will lose connectivity. To ensure client access, the devices should be configured with an address through, for example, an external DHCP service or assigning a static IP address.

• **Command:**
  
  DISABLE EBIPA{SERVER | INTERCONNECT} [ALL | <bay number> [{, | - } <bay number>]]

• **Description:**
  Disables the ability of the Onboard Administrator to give devices in the bays IP addresses using DHCP. If no bay numbers are specified, EBIPA is disabled for all bays. Devices in bays receive IP addresses from an external server.

• **Access level/Bay level:**
  Administrator, Operator

• **Restrictions:**
  None

**DISABLE EBIPAV6**

**CAUTION:** This command causes the affected devices to lose their current EBIPA-configured address. Any clients accessing the devices via that address will lose connectivity. To ensure client access, the devices should be configured with an address through, for example, an external DHCP service or assigning a static IP address.

• **Command:**
  
  DISABLE EBIPAV6{SERVER | INTERCONNECT} [ALL | <bay number> [{, | - } <bay number>]]

• **Description:**
  Disables the ability of the Onboard Administrator to give devices in the bays IPv6 addresses using DHCPv6. If no bay numbers are specified, then EBIPA IPv6 is disabled for all bays. Devices in bays receive IP addresses from an external server.

• **Access level/Bay level:**
  Administrator, Operator

• **Restrictions:**
  None

**ENABLE EBIPA**

• **Command:**
ENABLE EBIPA SERVER|INTERCONNECT [ALL | <bay number> [{ , | - } <bay number>]]

- **Description:**
  - Enables the Onboard Administrator to provide IP addresses to the devices in the bays using DHCP.
  - If no bay numbers are specified, then EBIPA is enabled for all bays.
  - If the device IP address has been configured by an external DHCP service, EBIPA settings (established by the SET EBIPA command) override the existing DHCP address. DHCP traffic from iLO and the interconnect modules that are EBIPA-enabled can no longer go outside the enclosure.

- **Access level/Bay level:**
  Administrator, Operator

- **Restrictions:**
  Before using this command you must set up all required EBIPA settings using SET EBIPA SERVER (on page 66) or SET EBIPA INTERCONNECT (on page 65). All iLOs and interconnect modules must be configured for DHCP support.

---

ENABLE EBIPAV6

- **Command:**
  ENABLE EBIPAV6 SERVER|INTERCONNECT [ALL | <bay number> [{ , | - } <bay number>]]

- **Description:**
  - Enables the Onboard Administrator to provide IPv6 addresses to the servers or interconnects in the bays using DHCPv6.
  - If no bay numbers are specified, then EBIPA IPv6 is enabled for all bays.
  - If the device IP address has been configured by an external DHCP service, EBIPA IPv6 settings (established by the SET EBIPAV6 command) override the existing DHCPv6 address. DHCP traffic from iLO and the interconnect modules can no longer go outside the enclosure.

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  Before using this command you must set up all required EBIPAV6 settings using SET EBIPAV6 SERVER (on page 68) or SET EBIPAV6 INTERCONNECT (on page 67). All iLOs and interconnect modules must be configured for DHCP support.

---

REMOVE EBIPA

- **Command:**
  REMOVE EBIPA SERVER|INTERCONNECT DNS [ALL | <ip address> [{ , | - } <bay number>]]

- **Description:**
  Removes an EBIPA DNS server IP address from the list of DNS servers for either server bays or interconnect bays. To remove all DNS server IP addresses corresponding to the specified bays, specify ALL instead of the IP address.
A bay number or range of bay numbers may be specified. If a bay number or range is not specified, or the keyword ALL is used instead, the command removes the DNS IP address from all interconnect or device bays where it exists.

- **Access level/Bay level:**
  Administrator, Operator

- **Restrictions:**
  The <ip address> must be in the form ###.###.###.###, where each ### ranges from 0 to 255.

**REMOVE EBIPAV6**

- **Command:**
  REMOVE EBIPAV6 { SERVER | INTERCONNECT } DNS {ALL | <ipv6 address>} [ALL | <bay number> [{, | - } <bay number>]]

- **Description:**
  Removes an EBIPA DNS server IPv6 address from the list of DNS servers for either server bays or interconnect bays. To remove all DNS server IP addresses corresponding to the specified bays, specify ALL instead of the IP address.
  
  A bay number or range of bay numbers may be specified. If a bay number or range is not specified, or the keyword ALL is used instead, the command removes the DNS IP address from all interconnect or device bays where it exists.

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  - A bay number or bay range may be specified. If no bay number or bay range is specified, the IPv6 DNS server is removed from all servers or interconnects.
  
  - The <ip address> must be in the form ####:####:####:####:####:####:####:####/###, where #### ranges from 0 to FFFF. A compressed version of the same IPv6 address is also supported.

**SAVE EBIPA**

- **Command:**
  SAVE EBIPA

- **Description:**
  Saves EBIPA settings for server bays or interconnect bays.

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  If script mode is enabled when EBIPA is configured (either by running EBIPA commands manually using the CLI or by downloading a configuration script using DOWNLOAD CONFIG (on page 92)), you must include the SAVE EBIPA command to ensure all EBIPA settings are saved.
SAVE EBIPAV6

- **Command:**
  
  ```text
  SAVE EBIPAV6
  ```

- **Description:**
  Saves EBIPA IPv6 settings for device or interconnect bays.

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  If script mode is enabled when EBIPA is configured (either by running EBIPA commands manually using the CLI or by downloading a configuration script using the command `DOWNLOAD CONFIG` (on page 92)), you must include the `SAVE EBIPA` command to ensure all EBIPA settings are saved.

SET EBIPA INTERCONNECT

⚠️ **CAUTION:** If EBIPA is enabled for the interconnect, changes to settings might result with loss of connectivity for clients currently accessing the interconnect using the previously assigned address.

- **Command:**
  
  ```text
  SET EBIPA INTERCONNECT {<IP address> <netmask>} | {NETMASK <netmask>} | {GATEWAY <gateway>} | {DOMAIN <domain>} | {NTP PRIMARY | SECONDARY <IP address>} [ALL | <bay number> [{- | ,} <bay number>]]
  ```

- **Description:**
  Sets EBIPA settings for interconnect bays. If the bay number or range of bay numbers is not specified, the settings are applied to all interconnect bays. You can specify an IP fixed address for a specific bay, or you can specify the starting IP fixed address for a range of bays, where EBIPA automatically assigns consecutive addresses to the bays in the range, starting with the specified address. You can specify a netmask (subnet mask), domain name, gateway, or NTP server for a specific bay or range of bays.

**NOTE:** The Onboard Administrator documentation refers to EBIPA IP addresses as "fixed IP addresses" or "fixed DHCP addresses," meaning that each of these addresses is an IP address permanently associated with a specific bay number independent of the actual device currently attached to the bay.

To clear the IP address and netmask values, use keywords `NONE NONE`. For example, to clear the address and netmask for bay 3, specify this command:

```text
SET EBIPA INTERCONNECT NONE NONE 3
```

To clear a specific bay, use the bay number.

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  - The `<IP address>` and `<netmask>` must be in the form `###.###.###.###`, where each `###` ranges from 0 to 255.
Do not use the 169.254.x.x range when configuring EBIPA-assigned addresses, as this network address range is reserved for use by the Onboard Administrator.

When specifying `<netmask>` and a range of bay numbers, specify a netmask that allows for enough available addresses on the associated subnet to accommodate all bays in the specified range. Specifying a subnet mask that does not meet that requirement causes the command to fail with the "No addresses left in the specified address range" error message.

The `<domain name>` is a string containing letters (a–z, A–Z), digits (0–9), or a dash (-).

The OA accepts domain name character strings subject to the following constraints:

- The string must be between 1 and 255 characters in length.
- The characters are case insensitive.
- The first character of the domain name must be alphanumeric, while the last character can be either alphanumeric or a period.
- The characters between the first and last character can be alphanumeric, dash or period.
- If one or more periods appear in the name, they are used to delimit labels.
- Labels are between 1 and 63 characters long and begin and end with an alphanumeric character.
- The last label is referred as the top-level domain and cannot consist of all numeric characters.

SET EBIPA SERVER

⚠️ CAUTION: If EBIPA is enabled for the server bay, this command causes a reset of the EBIPA-configured iLO. The iLO then attempts to obtain an IP address, which might result in loss of connectivity for clients currently accessing the iLO using the previously-assigned address.

- Command:
  ```
  SET EBIPA SERVER {<IP address> <netmask>} | {NETMASK <netmask>} | {GATEWAY <gateway>} | {DOMAIN <domain>} [ALL | <bay number> [{- | ,} <bay number>]]
  ```

- Description:
  Sets EBIPA settings for device server bays. If a bay number or range of bay numbers is not specified, the settings are applied to all device bays. You can specify an IP fixed address for a specific bay, or you can specify the starting IP fixed address for a range of bays, where EBIPA automatically assigns consecutive addresses to the bays in the range, starting with the specified address. You can specify a domain name or gateway for a specific bay or range of bays.

  **NOTE:** The Onboard Administrator documentation refers to EBIPA IP addresses as "fixed IP addresses" or "fixed DHCP addresses," meaning that each of these addresses is an IP address permanently associated with a specific bay number independent of the actual device currently attached to the bay.

  To clear the IP address and netmask (subnet mask) values, use keywords NONE NONE. For example, to clear the address and netmask for bay 3, specify this command:

  ```
  SET EBIPA SERVER NONE NONE 3
  ```

  To clear a specific bay, use the bay number.

- Access level/Bay level:
  OA administrator, OA operator
• **Restrictions:**
  
  o The `<IP address>` and `<netmask>` must be in the form `###.###.###.###`, where each `###` ranges from 0 to 255.
  
  o Do not use the 169.254.x.x range when configuring EBIPA-assigned addresses, as this network address range is reserved for use by the Onboard Administrator.
  
  o When specifying `<netmask>` and a range of bay numbers, specify a netmask that allows for enough available addresses on the associated subnet to accommodate all bays in the specified range. Specifying a subnet mask that does not meet that requirement causes the command to fail with the "No addresses left in the specified address range" error message.
  
  o The `<domain name>` is a string containing letters (a–z, A–Z), digits (0–9), or a dash (–). The OA accepts domain name character strings subject to the following constraints:
    - The string must be between 1 and 255 characters in length.
    - The characters are case insensitive.
    - The first character of the domain name must be alphanumeric, while the last character can be either alphanumeric or a period.
    - The characters between the first and last character can be alphanumeric, dash or period.
    - If one or more periods appear in the name, they are used to delimit labels.
    - Labels are between 1 and 63 characters long and begin and end with an alphanumeric character.
    - The last label is referred as the top-level domain and cannot consist of all numeric characters.

SET EBIPAV6 INTERCONNECT

⚠️ **CAUTION:** If EBIPA is enabled for the interconnect, changes to settings might result with loss of connectivity for clients currently accessing the interconnect using the previously assigned address.

• **Command:**

```
SET EBIPAV6 INTERCONNECT {<IPv6 address>{/prefix length}} | {DOMAIN <domain>} | {GATEWAY <gateway>} | [ALL | <bay number> [{- | ,} <bay number>]]
```

• **Description:**

Sets EBIPA IPv6 address settings for interconnect bays. If the bay number or a range of bay numbers is not specified, the settings will apply to all interconnects. You can specify an IPv6 fixed address for a specific bay, or you can specify the starting IPv6 fixed address for a range of bays, where EBIPA automatically assigns consecutive addresses to the bays in the range, starting with the specified address. (See the following example.) You can specify a domain name or gateway for a specific bay or range of bays.

**NOTE:** The Onboard Administrator documentation refers to EBIPA IP addresses as “fixed IP addresses” or “fixed DHCP addresses,” meaning that each of these addresses is an IP address permanently associated with a specific bay number independent of the actual device currently attached to the bay.

To clear the IPv6 address, use the keyword **NONE**. For example, to clear the address for bay 3, specify the following command:

```
SET EBIPAV6 INTERCONNECT NONE 3
```
Enclosure Bay IP Addressing commands

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  - The `<IPv6 address>` must be in the form 
    `####:####:####:####:####:####:####:####/###`, where #### ranges from 0 to FFFF. A 
    compressed version of the same IPv6 address is also supported.
  - The `/prefix length` ranges from 1 to 128. The prefix length is mandatory except when specifying the 
    gateway address.
  - Do not use the fe80::/10 prefix when configuring EBIPA-assigned addresses, as this network prefix 
    is reserved for link local SLAAC addresses.
  - When specifying the IPv6 subnet prefix and a range of bay numbers, specify a subnet prefix that 
    allows for enough available addresses on the associated subnet to accommodate all bays in the 
    range. Specifying a subnet prefix that does not meet that requirement causes the command to fail 
    with the "No addresses left in the specified address range" error message.
  - For the gateway, do not specify a prefix. The gateway is assumed reachable from within the 
    network.

  If the EBIPA IPv6 gateway is specified as a Link-Local address, the gateway will always be 
  configured on the enclosure device using this address. If the gateway is specified with any other 
  type of IPv6 address, the Onboard Administrator sends neighbor solicitation requests to identify the 
  Link-Local address of the gateway device. If the gateway does not exist or does not respond to 
  neighbor solicitation requests, no gateway is configured.
  - The `<domain name>` is a string containing letters (a–z, A–Z), digits (0–9), or a dash ({). To clear the 
    domain name, use an empty string enclosed by double quotes ("").
  - For EBIPA IPv6 fixed addresses to be successfully configured, the IPv6 protocol must be enabled. To 
    enable this setting, use  `ENABLE IPV6` (on page 95).

    The SLAAC and DHCPv6 settings have no effect on EBIPA IPv6 functionality.

- **Example:**
  OA-A0B3CCE63B65> set ebipav6 interconnect 4001::5aaa/64

  Entering anything other than 'YES' will result in the command not executing.

  It may take each interconnect several minutes to acquire the new settings.

  Are you sure you want to change the IPv6 address for the specified 
  interconnect bays? yes

  Successfully set interconnect bay # 1 to IPv6 address 4001::5aaa/64
  Successfully set interconnect bay # 2 to IPv6 address 4001::5aab/64
  Successfully set interconnect bay # 3 to IPv6 address 4001::5aac/64
  Successfully set interconnect bay # 4 to IPv6 address 4001::5aad/64

  For the IPv6 addresses to be assigned EBIPAv6 must be enabled.

---

**SET EBIPAV6 SERVER**

**CAUTION:** If EBIPA is enabled for the server bay, this command causes a reset of the 
EBIPA-configured iLO. The iLO then attempts to obtain an IP address, which might result in loss of 
connectivity for clients currently accessing the iLO using the previously-assigned address.
- **Command:**
  
  SET EBIPAV6 SERVER {<IPv6 address>/<prefix length}} | {DOMAIN <domain>}
  {GATEWAY <gateway>} | [ALL | <bay number> [{- | ,} <bay number>]]

- **Description:**
  
  Sets EBIPA IPv6 address settings for server bays and resets the iLO processor. If the bay number or range of bay numbers is not specified, the settings will be applied to all device bays. You can specify an IPv6 fixed address for a specific bay, or you can specify the starting IPv6 fixed address for a range of bays, where EBIPA automatically assigns consecutive addresses to the bays in the range, starting with the specified address. (See the following example.) You can specify a domain name or gateway for a specific bay or range of bays.

  **NOTE:** The Onboard Administrator documentation refers to EBIPA IP addresses as “fixed IP addresses” or “fixed DHCP addresses,” meaning that each of these addresses is an IP address permanently associated with a specific bay number independent of the actual device currently attached to the bay.

  To clear the IPv6 address, use the keyword NONE. For example, to clear the address for bay 3, specify the following command:
  
  SET EBIPAV6 SERVER NONE 3

- **Access level/Bay level:**
  
  OA administrator, OA operator

- **Restrictions:**
  
  - The <IPv6 address> must be in the form
    
    ####:####:####:####:####:####:####:####/####, where #### ranges from 0 to FFFF. A compressed version of the same IPv6 address is also supported.

  - The /prefix length ranges from 1 to 128. The prefix length is mandatory except when specifying the address of the gateway.

  - Do not use the fe80::/10 prefix when configuring EBIPA-assigned addresses, as this network prefix is reserved for link local SLAAC addresses.

  - When specifying the IPv6 subnet prefix and a range of bay numbers, specify a subnet prefix that allows for enough available addresses on the associated subnet to accommodate all bays in the range. Specifying a subnet prefix that does not meet that requirement causes the command to fail with the “No addresses left in the specified address range” error message.

  - For the gateway, do not specify a prefix. The gateway is assumed reachable from within the network.

    If the EBIPA IPv6 gateway is specified as a Link-Local address, the gateway will always be configured on the enclosure device using this address. If the gateway is specified with any other type of IPv6 address, the Onboard Administrator sends neighbor solicitation requests to identify the Link-Local address of the gateway device. If the gateway does not exist or does not respond to neighbor solicitation requests, no gateway is configured.

  - The <domain name> is a string containing letters (a–z, A–Z), digits (0–9), or a dash (-). To clear the domain name, use an empty string enclosed by double quotes (“”).

  - For EBIPA IPv6 fixed addresses to be successfully configured, the IPv6 protocol must be enabled. To enable this setting, use the command ENABLE IPV6 (on page 95).

    The SLAAC and DHCPv6 settings have no effect on EBIPA IPv6 functionality.

- **Example:**
Enclosure Bay IP Addressing commands

OA-A0B3CCE63B65> set ebipav6 server 4001::4bbc/64 all

Entering anything other than 'YES' will result in the command not executing.

Changing the IPv6 address for device (iLO) bays that are enabled causes the iLOs in those bays to be reset.

Are you sure you want to change the IPv6 address for the specified device (iLO) bays? yes
Successfully set device (iLO) bay # 1 to IPv6 address 4001::4bbc/64
Successfully set device (iLO) bay # 2 to IPv6 address 4001::4bbd/64
Successfully set device (iLO) bay # 3 to IPv6 address 4001::4bbe/64
Successfully set device (iLO) bay # 4 to IPv6 address 4001::4bbf/64
Successfully set device (iLO) bay # 5 to IPv6 address 4001::4bc0/64
Successfully set device (iLO) bay # 6 to IPv6 address 4001::4bc1/64
Successfully set device (iLO) bay # 7 to IPv6 address 4001::4bc2/64
Successfully set device (iLO) bay # 8 to IPv6 address 4001::4bc3/64
Successfully set device (iLO) bay #1A to IPv6 address 4001::4bc4/64
Successfully set device (iLO) bay #2A to IPv6 address 4001::4bc5/64
Successfully set device (iLO) bay #3A to IPv6 address 4001::4bc6/64
Successfully set device (iLO) bay #4A to IPv6 address 4001::4bc7/64
Successfully set device (iLO) bay #5A to IPv6 address 4001::4bc8/64
Successfully set device (iLO) bay #6A to IPv6 address 4001::4bc9/64
Successfully set device (iLO) bay #7A to IPv6 address 4001::4bca/64
Successfully set device (iLO) bay #8A to IPv6 address 4001::4bcb/64
Successfully set device (iLO) bay #1B to IPv6 address 4001::4bcc/64
Successfully set device (iLO) bay #2B to IPv6 address 4001::4bcd/64
Successfully set device (iLO) bay #3B to IPv6 address 4001::4bce/64
Successfully set device (iLO) bay #4B to IPv6 address 4001::4bcf/64
Successfully set device (iLO) bay #5B to IPv6 address 4001::4bd0/64
Successfully set device (iLO) bay #6B to IPv6 address 4001::4bd1/64
Successfully set device (iLO) bay #7B to IPv6 address 4001::4bd2/64
Successfully set device (iLO) bay #8B to IPv6 address 4001::4bd3/64

For the IPv6 addresses to be assigned EBIPA v6 must be enabled.

SHOW EBIPA

- **Command:**
  SHOW EBIPA

- **Description:**
  Displays EBIPA information

- **Access level/Bay level:**
  Administrator, Operator, User

- **Restrictions:**
  None

- **Example:**
  OA-0018FE27577F> SHOW EBIPA

  EBIPA Device Server Settings
<table>
<thead>
<tr>
<th>Bay Enabled</th>
<th>EBIPA/Current</th>
<th>Netmask</th>
<th>Gateway</th>
<th>DNS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Yes</td>
<td>111.22.211.111</td>
<td>255.255.0.0</td>
<td>111.22.0.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>111.22.211.111</td>
<td>111.22.0.2</td>
</tr>
<tr>
<td>1A</td>
<td>Yes</td>
<td>111.22.211.119</td>
<td>255.255.0.0</td>
<td>111.22.0.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>111.22.211.119</td>
<td>111.22.0.2</td>
</tr>
<tr>
<td>1B</td>
<td>Yes</td>
<td>111.22.211.127</td>
<td>255.255.0.0</td>
<td>111.22.0.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>111.22.211.127</td>
<td>111.22.0.2</td>
</tr>
<tr>
<td>2</td>
<td>Yes</td>
<td>111.22.211.112</td>
<td>255.255.0.0</td>
<td>111.22.0.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>111.22.211.112</td>
<td>111.22.0.2</td>
</tr>
<tr>
<td>2A</td>
<td>Yes</td>
<td>111.22.211.120</td>
<td>255.255.0.0</td>
<td>111.22.0.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>111.22.211.120</td>
<td>111.22.0.2</td>
</tr>
<tr>
<td>2B</td>
<td>Yes</td>
<td>111.22.211.128</td>
<td>255.255.0.0</td>
<td>111.22.0.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>111.22.211.128</td>
<td>111.22.0.2</td>
</tr>
<tr>
<td>3</td>
<td>Yes</td>
<td>111.22.211.113</td>
<td>255.255.0.0</td>
<td>111.22.0.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>111.22.211.113</td>
<td>111.22.0.2</td>
</tr>
<tr>
<td>3A</td>
<td>Yes</td>
<td>111.22.211.121</td>
<td>255.255.0.0</td>
<td>111.22.0.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>111.22.211.121</td>
<td>111.22.0.2</td>
</tr>
<tr>
<td>3B</td>
<td>Yes</td>
<td>111.22.211.129</td>
<td>255.255.0.0</td>
<td>111.22.0.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>111.22.211.129</td>
<td>111.22.0.2</td>
</tr>
<tr>
<td>4</td>
<td>Yes</td>
<td>111.22.211.114</td>
<td>255.255.0.0</td>
<td>111.22.0.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>111.22.211.114</td>
<td>111.22.0.2</td>
</tr>
<tr>
<td>4A</td>
<td>Yes</td>
<td>111.22.211.122</td>
<td>255.255.0.0</td>
<td>111.22.0.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>111.22.211.122</td>
<td>111.22.0.2</td>
</tr>
<tr>
<td>4B</td>
<td>Yes</td>
<td>111.22.211.130</td>
<td>255.255.0.0</td>
<td>111.22.0.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>111.22.211.130</td>
<td>111.22.0.2</td>
</tr>
<tr>
<td>5</td>
<td>Yes</td>
<td>111.22.211.115</td>
<td>255.255.0.0</td>
<td>111.22.0.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>111.22.211.115</td>
<td>111.22.0.2</td>
</tr>
<tr>
<td>5A</td>
<td>Yes</td>
<td>111.22.211.123</td>
<td>255.255.0.0</td>
<td>111.22.0.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>111.22.211.123</td>
<td>111.22.0.2</td>
</tr>
<tr>
<td>Bay</td>
<td>Enabled</td>
<td>EBIPA/Current</td>
<td>Netmask</td>
<td>Gateway</td>
</tr>
<tr>
<td>-----</td>
<td>---------</td>
<td>---------------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>5B</td>
<td>Yes</td>
<td>111.22.211.131</td>
<td>255.255.0.0</td>
<td>111.22.0.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>test.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Yes</td>
<td>111.22.211.122</td>
<td>255.255.0.0</td>
<td>111.22.0.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>test.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6A</td>
<td>Yes</td>
<td>111.22.211.124</td>
<td>255.255.0.0</td>
<td>111.22.0.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>test.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6B</td>
<td>Yes</td>
<td>111.22.211.132</td>
<td>255.255.0.0</td>
<td>111.22.0.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>test.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Yes</td>
<td>111.22.211.117</td>
<td>255.255.0.0</td>
<td>111.22.0.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>test.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7A</td>
<td>Yes</td>
<td>111.22.211.125</td>
<td>255.255.0.0</td>
<td>111.22.0.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>test.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7B</td>
<td>Yes</td>
<td>111.22.211.133</td>
<td>255.255.0.0</td>
<td>111.22.0.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>test.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Yes</td>
<td>111.22.211.118</td>
<td>255.255.0.0</td>
<td>111.22.0.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>test.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8A</td>
<td>Yes</td>
<td>111.22.211.126</td>
<td>255.255.0.0</td>
<td>111.22.0.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>test.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8B</td>
<td>Yes</td>
<td>111.22.211.134</td>
<td>255.255.0.0</td>
<td>111.22.0.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>test.com</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

EBIPA Device Interconnect Settings

<table>
<thead>
<tr>
<th>Bay Enabled</th>
<th>EBIPA/Current</th>
<th>Netmask</th>
<th>Gateway</th>
<th>DNS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Yes</td>
<td>111.22.211.183</td>
<td>255.255.0.0</td>
<td>111.22.0.1</td>
<td>111.22.0.1</td>
</tr>
<tr>
<td>2.3.4.5</td>
<td>testIO.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 Yes</td>
<td>111.22.211.184</td>
<td>255.255.0.0</td>
<td>111.22.0.1</td>
<td>111.22.0.1</td>
</tr>
<tr>
<td>2.3.4.5</td>
<td>testIO.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 Yes</td>
<td>111.22.211.185</td>
<td>255.255.0.0</td>
<td>111.22.0.1</td>
<td>111.22.0.1</td>
</tr>
<tr>
<td>2.3.4.5</td>
<td>testIO.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 Yes</td>
<td>111.22.211.186</td>
<td>255.255.0.0</td>
<td>111.22.0.1</td>
<td>111.22.0.1</td>
</tr>
<tr>
<td>2.3.4.5</td>
<td>testIO.com</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SHOW EBIPAV6

- **Command:**
  
  SHOW EBIPAV6

- **Description:**
  
  Displays EBIPA IPv6 information

- **Access level/Bay level:**
  
  Administrator, Operator, User

- **Restrictions:**
  
  None

- **Example:**
  
  OA-0018FE27577F> SHOW EBIPAV6

  EBIPAv6 Device Blades Settings

  Bay:  1  Enabled: Yes
  EBIPA:  1111::222:10:2/64
  Current: (Not Set)
  Gateway: (Not Set)
  DNS 1:  1111::1
  DNS 2:  1111::5
  DNS 3:  (Not Set)
  Domain:  bladeslab.com

  Bay:  1B  Enabled: No
  EBIPA:  (Not Set)
  Current: (Not Set)
  Gateway: (Not Set)
  DNS 1:  (Not Set)
  DNS 2:  (Not Set)
  DNS 3:  (Not Set)
  Domain:  (Not Set)

  Bay:  2  Enabled: Yes
  EBIPA:  1111::222:10:2/64
  Current: (Not Set)
  Gateway: (Not Set)
  DNS 1:  1111::1
  DNS 2:  1111::5
  DNS 3:  (Not Set)
  Domain:  bladeslab.com

  Bay:  2A  Enabled: No
  EBIPA:  (Not Set)
  Current: (Not Set)
  Gateway: (Not Set)
  DNS 1:  (Not Set)
  DNS 2:  (Not Set)
  DNS 3:  (Not Set)
  Domain:  (Not Set)

  Bay:  2B  Enabled: No
  EBIPA:  (Not Set)
Bay: 3 Enabled: Yes
EBIPA: 1111::222:10:3/64
Current: (Not Set)
Gateway: (Not Set)
DNS 1: 1111::1
DNS 2: 1111::5
DNS 3: (Not Set)
Domain: bladeslab.com

Bay: 3A Enabled: No
EBIPA: (Not Set)
Current: (Not Set)
Gateway: (Not Set)
DNS 1: (Not Set)
DNS 2: (Not Set)
DNS 3: (Not Set)
Domain: (Not Set)

Bay: 3B Enabled: No
EBIPA: (Not Set)
Current: (Not Set)
Gateway: (Not Set)
DNS 1: (Not Set)
DNS 2: (Not Set)
DNS 3: (Not Set)
Domain: (Not Set)

Bay: 4 Enabled: Yes
EBIPA: 1111::222:10:4/64
Current: (Not Set)
Gateway: (Not Set)
DNS 1: 1111::1
DNS 2: 1111::5
DNS 3: (Not Set)
Domain: bladeslab.com

Bay: 4A Enabled: No
EBIPA: (Not Set)
Current: (Not Set)
Gateway: (Not Set)
DNS 1: (Not Set)
DNS 2: (Not Set)
DNS 3: (Not Set)
Domain: (Not Set)

Bay: 4B Enabled: No
EBIPA: (Not Set)
Current: (Not Set)
Gateway: (Not Set)
DNS 1: (Not Set)
DNS 2: (Not Set)
DNS 3: (Not Set)
Bay: 5
   Enabled: Yes
   EBIPA: 1111::222:10:5/64
   Current: (Not Set)
   Gateway: (Not Set)
   DNS 1: 1111::1
   DNS 2: 1111::5
   DNS 3: (Not Set)
   Domain: bladeslab.com

Bay: 5A
   Enabled: No
   EBIPA: (Not Set)
   Current: (Not Set)
   Gateway: (Not Set)
   DNS 1: (Not Set)
   DNS 2: (Not Set)
   DNS 3: (Not Set)
   Domain: (Not Set)

Bay: 5B
   Enabled: No
   EBIPA: (Not Set)
   Current: (Not Set)
   Gateway: (Not Set)
   DNS 1: (Not Set)
   DNS 2: (Not Set)
   DNS 3: (Not Set)
   Domain: (Not Set)

Bay: 6
   Enabled: Yes
   EBIPA: 1111::222:10:6/64
   Current: (Not Set)
   Gateway: (Not Set)
   DNS 1: 1111::1
   DNS 2: 1111::5
   DNS 3: (Not Set)
   Domain: bladeslab.com

Bay: 6A
   Enabled: No
   EBIPA: (Not Set)
   Current: (Not Set)
   Gateway: (Not Set)
   DNS 1: (Not Set)
   DNS 2: (Not Set)
   DNS 3: (Not Set)
   Domain: (Not Set)

Bay: 6B
   Enabled: No
   EBIPA: (Not Set)
   Current: (Not Set)
   Gateway: (Not Set)
   DNS 1: (Not Set)
   DNS 2: (Not Set)
   DNS 3: (Not Set)
   Domain: (Not Set)

Bay: 7
   Enabled: Yes
   EBIPA: 1111::222:10:7/64
   Current: (Not Set)
Gateway: (Not Set)
DNS 1:  1111::1
DNS 2:  1111::5
DNS 3:  (Not Set)
Domain:  bladeslab.com

------------------------------------------------------------------------
Bay:  7A  Enabled: No
EBIPA:   (Not Set)
Current: (Not Set)
Gateway: (Not Set)
DNS 1:   (Not Set)
DNS 2:   (Not Set)
DNS 3:   (Not Set)
Domain:  (Not Set)

------------------------------------------------------------------------
Bay:  7B  Enabled: No
EBIPA:   (Not Set)
Current: (Not Set)
Gateway: (Not Set)
DNS 1:   (Not Set)
DNS 2:   (Not Set)
DNS 3:   (Not Set)
Domain:  (Not Set)

------------------------------------------------------------------------
Bay:  8   Enabled: Yes
EBIPA:   1111::222:10:8/64
Current: (Not Set)
Gateway: (Not Set)
DNS 1:   1111::1
DNS 2:   1111::5
DNS 3:   (Not Set)
Domain:  bladeslab.com

------------------------------------------------------------------------
Bay:  8A  Enabled: No
EBIPA:   (Not Set)
Current: (Not Set)
Gateway: (Not Set)
DNS 1:   (Not Set)
DNS 2:   (Not Set)
DNS 3:   (Not Set)
Domain:  (Not Set)

------------------------------------------------------------------------
Bay:  8B  Enabled: No
EBIPA:   (Not Set)
Current: (Not Set)
Gateway: (Not Set)
DNS 1:   (Not Set)
DNS 2:   (Not Set)
DNS 3:   (Not Set)
Domain:  (Not Set)
Enclosure network configuration commands

ADD OA ADDRESS IPV6

- **Command:**
  
  ADD OA ADDRESS IPV6 [{<bay number>}| ACTIVE | STANDBY] <ipv6 address/prefix length>

- **Description:**
  Adds an IPv6 static address for the Onboard Administrator. If IPv6 is enabled, this setting takes effect immediately. If none of the optional arguments are specified (Onboard Administrator bay number, ACTIVE, or STANDBY), the command defaults to the active Onboard Administrator.

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  - The prefix length is mandatory.
  - The `<ip address>` must be in the form ####:####:####:####:####:####:####:####/###, where each #### ranges from 0 to FFFF. A compressed version of the same IPv6 address is also supported. The prefix /### ranges from 1 to 128.
  - Do not specify a Link Local Address as the IPv6 static address.

ADD OA DNS

- **Command:**
  ADD OA DNS [bay number] <ip address>

- **Description:**
  - Adds an IP address of a DNS server to the list of DNS servers.
  - If a bay number is not specified, then the command defaults to the current (local) Onboard Administrator.
  - The Onboard Administrator can use up to six DNS servers to look up an IP address: two IPv4 DNS servers (either static or DHCP assigned, but not both) and four IPv6 DNS servers (static or DHCP assigned, or both). The Onboard Administrator uses the DNS servers in the following order:
    - IPv4 DNS server 1 (static)
    - IPv6 DNS server 1 (static)
    - IPv4 DNS server 2 (static)
    - IPv6 DNS server 2 (static)
    - IPv4 DNS server 1 (DHCP assigned)
    - IPv6 DNS server 1 (DHCP assigned)
    - IPv4 DNS server 2 (DHCP assigned)
IPv6 DNS server 2 (DHCP assigned)

If any of the DNS servers in this list are not configured, the DNS servers that follow them in the list move up in order, accordingly. For example, if the DHCP-assigned IPv4 DNS servers 1 and 2 are not configured, the two DHCP-assigned IPv6 DNS servers move up to 5th and 6th in the list. As noted previously, IPv4 DNS servers can either be static or DHCP assigned, not both; so the maximum number of DNS servers that the Onboard Administrator can use is 6.

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  - A maximum of two static IPv4 DNS servers can be added.
  - The `<ip address>` must be in the form ###.###.###.###, where each ### ranges from 0 to 255.

## ADD OA DNS IPV6

- **Command:**
  ADD OA DNS IPV6 [<bay number>] <ipv6 address{/prefix length}>

- **Description:**
  - Adds an IPv6 address of a DNS server to the list of DNS servers.
  - The network prefix length is optional.
  - If a bay number is not specified, then the command defaults to the current (local) Onboard Administrator.
  - The Onboard Administrator can use up to six DNS servers to look up an IP address: two IPv4 DNS servers (either static or DHCP assigned, but not both) and four IPv6 DNS servers (static or DHCP assigned, or both). The Onboard Administrator uses the DNS servers in the following order:
    - IPv4 DNS server 1 (static)
    - IPv6 DNS server 1 (static)
    - IPv4 DNS server 2 (static)
    - IPv6 DNS server 2 (static)
    - IPv4 DNS server 1 (DHCP assigned)
    - IPv6 DNS server 1 (DHCP assigned)
    - IPv4 DNS server 2 (DHCP assigned)
    - IPv6 DNS server 2 (DHCP assigned)
  - If any of the DNS servers in this list are not configured, the DNS servers that follow them in the list move up in order, accordingly. For example, if the DHCP-assigned IPv4 DNS servers 1 and 2 are not configured, the two DHCP-assigned IPv6 DNS servers move up to 5th and 6th in the list. As noted previously, IPv4 DNS servers can either be static or DHCP assigned, not both; so the maximum number of DNS servers that the Onboard Administrator can use is 6.

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
A maximum of two DNS servers can be added.

The `<ipv6 address>` must be in the form `####:####:####:####:####:####:####:####` or `####:####:####:####:####:####:####:####/###` (with an optional prefix), where each `####` ranges from 0 to FFFF. The prefix `/###` ranges from 1 to 128. A compressed version of the same IPv6 address is also supported.

**ADD OA ROUTE IPV6**

- **Command:**
  
  ADD OA ROUTE IPV6 [<bay number> | ACTIVE | STANDBY] <route destination> <route gateway>

- **Description:**
  
  o Adds an IPv6 static route to the Onboard Administrator routing table.
  o The static route defines an explicit path that the Onboard Administrator uses to reach an external network through a gateway. In a static network configuration, the static route removes the need to configure the router to send route information via router advertisements.
  
  If router advertisements are active in the network, and the default gateway is already configured, the router informs all nodes about the available static routes, thereby making manual configuration of static routes unnecessary.
  o If you do not specify the Onboard Administrator (<bay number>, ACTIVE, or STANDBY), the command defaults to the Onboard Administrator from which the command is issued.
  o The `<route destination>` specifies the IPv6 address of the static route, while the `<route gateway>` specifies the IPv6 address of the gateway using this static route.

  ▲ **CAUTION:** Adding or removing a static route might close client connections to the Onboard Administrator.

- **Access level/Bay level:**
  
  OA administrator, OA operator

- **Restrictions:**
  
  o A maximum of three static routes can be added.
  o The `<route destination>` IPv6 address must be in the form `####:####:####:####:####:####:####:####` (with a prefix), where each `####` ranges from 0 to FFFF. The prefix `/###` ranges from 1 to 128. A compressed version of the same IPv6 address is also supported.
  o The `<route gateway>` IPv6 address must be in the form `####:####:####:####:####:####:####:####` where `####` ranges from 0 to FFFF. Do not specify a prefix. A compressed version of the same IPv6 address is also supported.
  o The gateway must be reachable from both the Onboard Administrator network and the external network.

**ADD SSHKEY**

- **Command:**
  
  ADD SSHKEY <end marker> <\n> <key> <\n> <end marker>
• **Description:**
  Adds an SSH key or keys to the Administrator local account. Multiple SSH keys can be concatenated in the string. To add a key:
  a. Start with a string that does not appear within the key (the end marker).
  b. Insert a newline character by pressing **Enter**.
  c. Paste the certificate on the command line.
  d. Insert a newline character by pressing **Enter**.
  e. Insert the end marker.
  f. Issue the command by pressing **Enter**.

Failure to give a proper end marker before and after the key might cause the interface to wait for the appropriate end marker indefinitely.

• **Access level/Bay level:**
  OA administrator

• **Restrictions:**
  o This command is only available for the Administrator local account.
  o This command works only in script mode.
  o The SSHKEY string is limited to 8192 bytes.
  o This command is only valid in script mode.
  o When the Onboard Administrator is operating in FIPS Mode, certificates must have a minimum RSA key length of 2048 bits, and the signature hash algorithm must be SHA1, SHA-224, SHA-256, SHA-384, or SHA-512.

---

**ADD SNMP TRAPRECEIVER**

• **Command:**
  
  ADD SNMP TRAPRECEIVER <host> ["<community name>"]

• **Description:**
  o This command adds a new trap receiver to the SNMP configuration. As a result, SNMP v1 traps are sent to the specified SNMP v1/v2c trap receiver address. (The Onboard Administrator GUI refers to a trap as an "Alert", and the trap receiver as the "Alert Destination.")
  o By default, SNMP v1 traps are sent to destination port 162.
  o The **<host>** value is the management station IP address or DNS name, specified in [protocol:]destination[:port] format.
    — The **destination** is mandatory. Specify an IPv4 address, IPv6 address, or a DNS name.
    — The **protocol** is optional. For an IPv4 destination, it is **udp**. For an IPv6 destination, it may be **udp6**, **udpv6**, or **udpipv6**.
    — The **port** is optional and can be any valid and available decimal port number from 1 to 65535. If port is specified for an IPv6 address, the IPv6 address must be enclosed in brackets. The default port is 162. For example, to specify port 162, use this format (the enclosing brackets are required): [#####:#####:#####]:162.
  o The SNMP Trap community string is set to **public** or the optional **<community name>**.
• **Access level/Bay level:**
  OA administrator, OA operator

• **Restrictions:**
  o A maximum of eight IP addresses can be added to receive SNMP traps.
  o SNMP v1/v2c trap receivers are supported with this command. For support of v3 trap receivers, use the command `ADD SNMP TRAPRECEIVER V3` (on page 81).
  o An IPv4 address must be in the form ###.###.###.###, where each ### ranges from 0 to 255.
  o An IPv6 address must be in the form ####:####:####:####:####:####:####:####, where each #### ranges from 0 to FFFF. A compressed version of the same IPv6 address is also supported. Do not include the prefix.
  o The DNS name, if specified, must be 1 to 64 characters in length, and may include any alphanumeric characters and the dash (-).
  o The `<community_name>` string, if specified, must be 1 to 20 characters in length. Acceptable characters include any printable character excluding quotes and newlines.

**ADD SNMP TRAPRECEIVER V3**

• **Command:**

```
ADD SNMP TRAPRECEIVER V3 {<host> <user name>[ENGINEID "<engineid>"] [NOAUTHNOPRIV|AUTHNOPRIV|AUTHPRIV] [INFORM]}
```

• **Description:**
  o This command adds a new trap receiver to the SNMP configuration. As a result, SNMP v3 traps are sent to the specified SNMP v3 trap receiver. (The Onboard Administrator GUI refers to a trap as an "Alert", and the trap receiver as the "Alert Destination").
  o This command is an extension of the existing `ADD SNMP TRAPRECEIVER` command. The additional `V3` parameter indicates this command is an SNMP v3 trap and requires additional parameters.
  o The `<host>` value is the management station IP address or DNS name, specified in `[protocol:]destination[:port]` format.
    — The `destination` is mandatory. Specify an IPv4 address, IPv6 address, or a DNS name.
    — The `protocol` is optional. For an IPv4 destination, it may be `udp` or `tcp`. For an IPv6 destination, it may be `tcp6`, `tcpv6`, or `tcpipv6`; or `udp6`, `udpv6`, or `udppipv6`.
    — The `port` is optional and can be any valid and available decimal port number from 1 to 65535. If `port` is specified for an IPv6 address, the IPv6 address must be enclosed in brackets. The default port is 162. For example, to specify port 162, use this format (the enclosing brackets are required): [#####:#####]:162.
  o The `<user name>` parameter specifies the SNMP v3 user account used for sending the trap/inform. The account does not have to exist at the time the trap receiver is created. However, when a trap is sent, access will not be authorized by the trap receiver host without the user account credentials. To add a user account, use the command `ADD SNMP USER` (on page 82).
  o If `ENGINEID` is not specified, the local engine ID is used. The `<engineid>` consists of prefix 0x and an even number of up to 64 hexadecimal digits.
The security level may be NOAUTHNOPRIV (no authentication, no encryption), AUTHNOPRIV (authentication, no encryption), or AUTHPRIV (authentication and encryption). The default is AUTHNOPRIV.

INFORM indicates an acknowledged SNMP v3 inform message instead of a trap. By default, the event is a trap.

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  - Eight v1/2c traps and eight v3 traps are allowed, for a total of 16 traps.
  - An IPv4 address must be in the form ###.###.###.###, where each ### ranges from 0 to 255.
  - An IPv6 address must be in the form ####:####:####:####:####:####:####:####, where each #### ranges from 0 to FFFF. A compressed version of the same IPv6 address is also supported. Do not include the prefix.
  - The DNS name, if specified, must be 1 to 64 characters in length, and may include any alphanumeric characters and the dash (-).

### ADD SNMP USER

- **Command:**
  ADD SNMP USER "<username>" {MD5|SHA1} "<auth passphrase"> {DES|AES128} ["<priv passphrase">] [ENGINEID <"engineID"> | [noAuthNoPriv|authNoPriv|authPriv]] ["RW"]

- **Description:**
  - Creates a new user to be used for SNMPv3 queries, traps, and informs.
  - A commented out version if this command is included in the configuration script. The original passwords cannot be retrieved. Therefore, the original command cannot be issued.

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  - Each user name/engine ID pair must be unique.
  - Up to ten distinct users are allowed.
  - When FIPS Mode is enabled, DES and MD5 are not allowed, and users are limited to read-only access.

- **Command parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>An alphanumeric string up to 32 characters in length</td>
</tr>
<tr>
<td>MD5 or SHA1</td>
<td>Use the MD5 or SHA1 algorithm to encode the authorization passphrase. MD5 is not allowed when FIPS Mode is enabled.</td>
</tr>
<tr>
<td>Auth passphrase</td>
<td>Authorization passphrase used to sign operations. This entry must be at least eight characters in length.</td>
</tr>
<tr>
<td>DES or AES128</td>
<td>Use the DES or AES128 algorithm to encode the privacy passphrase. DES is not allowed when FIPS Mode is enabled.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Privacy passphrase</td>
<td>Privacy passphrase used to encrypt operations. This entry must be at least eight characters in length. If not specified, the authorization passphrase is used.</td>
</tr>
</tbody>
</table>
| noAuthNoPriv | authNoPriv | authPriv | Only applies to local users. A minimal level of security is required for operation. By default, the operation is required to be signed but not encrypted (authNoPriv).  
  - noAuthNoPriv—Allows unauthenticated operations  
  - authNoPriv—Requires authentication  
  - authPriv—Required encryption |
| ENGINEID                         | Sets the engine ID for the user account. If set, the engine ID must be a series of hexadecimal characters, up to 32 bytes or 64 characters in length. This parameter is used for creating remote accounts used with INFORM messages. |
| RW                               | Specifies that this user has read/write access to the OID tree. If not specified, the user has read-only access. |

### ADD TRUSTED HOST

- **Command:**
  
  ADD TRUSTED HOST <ip address>

- **Description:**
  
  Adds a new IPv4 or IPv6 address to the list of addresses being handled by the IP Security feature.

- **Access level /Bay level:**
  
  OA administrator

- **Restrictions:**
  
  - You can add a maximum of five IP addresses to the IP Manager.
  - When specifying an IPv6 address, do not specify the prefix length.

⚠️ **CAUTION:** When using the Trusted Hosts feature in an environment with multiple enclosures connected via enclosure link cables, ensure that all linked enclosures have the same Trusted Hosts settings. Linked enclosures that do not have the same Trusted Hosts settings may allow a web GUI user to access a protected enclosure from a non-trusted client.

⚠️ **CAUTION:** RFC 4941 describes an IPv6 SLAAC extension that allows for generation of global-scope temporary IPv6 addresses using interface identifiers that change over time. When an OS that supports RFC 4941 reboots or the current address expires, a new temporary IPv6 address is generated. Windows 7 is an example of an OS that supports RFC 4941. With trusted hosts enabled, if you are accessing the Onboard Administrator from a client hosted on an OS with RFC 4941 support, a reboot of the client OS can result in the inability to reconnect to the Onboard Administrator. The connection fails because the client’s new temporary IPv6 address does not match the IPv6 address configured for the client in the Trusted Addresses list. To avoid this issue, either disable generation of global-scope temporary IPv6 addresses in the OS, or reconfigure the Trusted Host IP address with the newly generated client IPv6 address.
CLEAR LOGIN_BANNER_TEXT

- **Command:**
  ```
  CLEAR LOGIN_BANNER_TEXT
  ```
- **Description:**
  Clears the currently configured login banner text.
- **Access level/Bay level:**
  OA administrator
- **Restrictions:**
  Clearing the login banner text disables the login banner option.

CLEAR NTP

- **Command:**
  ```
  CLEAR NTP {PRIMARY | SECONDARY}
  ```
- **Description:**
  Disables access to the Primary or Secondary NTP server
- **Access level/Bay level:**
  OA administrator, OA operator
- **Restrictions:**
  Clearing the Primary NTP server disables NTP.

CLEAR SSHKEY

- **Command:**
  ```
  CLEAR SSHKEY
  ```
- **Description:**
  Removes the authorized key file used for SSH login
- **Access level/Bay level:**
  Administrator
- **Restrictions:**
  None

CLEAR VCMODE

- **Command:**
  ```
  CLEAR VCMODE
  ```
- **Description:**
  Clears Virtual Connect Mode settings.
OA Administrator
OA Bays

- **Restrictions:**
  - All servers in the enclosure should be powered off before clearing the VCMODE.
  - The enclosure will no longer be managed by Virtual Connect, and servers will revert to default Ethernet MAC and Fibre Channel WWN assignments. Virtual Connect might disconnect the servers from Ethernet networks and Fibre Channel fabrics.

### DISABLE ALERTMAIL

- **Command:**
  
  DISABLE ALERTMAIL

- **Description:**
  Disables the sending of emails when events occur

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  None

### DISABLE DHCPV6

- **Command:**
  
  DISABLE DHCPV6

- **Description:**
  Disables DHCPv6 mode for management interfaces of all devices in the enclosure. With DHCPv6 disabled, the IPv6 and DNS addresses are not obtained from the DHCPv6 Server. This setting takes effect immediately.

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  None

**NOTE:** When DHCPv6 mode is disabled, the respective DHCPv6 addresses of the iLOs in the enclosure are retained until these addresses expire automatically based on their respective configurations. A manual reset of the iLO releases these addresses immediately.

### DISABLE ENCLOSURE_ILO_FEDERATION_SUPPORT

- **Command:**
  
  DISABLE ENCLOSURE_ILO_FEDERATION_SUPPORT

- **Description:**
Disables the Onboard Administrator support required to allow peer-to-peer network communication necessary for iLO Federation among suitably capable iLOs within the enclosure. To enable this support, use **ENABLE ENCLOSURE_ILO_FEDERATION_SUPPORT** (on page 93).

- **Access level/Bay level:**
  - OA administrator, OA operator
- **Restrictions:**
  - None

**DISABLE ENCLOSURE_IP_MODE**

- **Command:**
  - DISABLE ENCLOSURE_IP_MODE
- **Description:**
  - Disables Enclosure IP Mode.
    - Active and Standby Onboard Administrators retain their current IP addresses.
    - After disabling Enclosure IP Mode and a takeover occurs, there will no longer be a single IP address for the enclosure.
- **Access level/Bay level:**
  - OA administrator, Operator
- **Restrictions:**
  - None

**DISABLE HTTPS**

- **Command:**
  - DISABLE HTTPS
- **Description:**
  - Disables HTTPS access to the Onboard Administrator, which prevents access to the web-based user interface
- **Access level/Bay level:**
  - OA administrator, OA operator
- **Restrictions:**
  - None

**DISABLE FQDN_LINK_SUPPORT**

- **Command:**
  - DISABLE FQDN_LINK_SUPPORT
- **Description:**
Disables the Onboard Administrator from displaying an FQDN-based web address link in addition to the usual IP-based web address links used for accessing an iLO or interconnect from the Onboard Administrator GUI.

When the FQDN setting is disabled, the FQDN links of all the enclosure devices are removed from the Onboard Administrator and hence are not displayed.

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  None

### DISABLE IPV6

- **Command:**
  DISABLE IPV6

- **Description:**
  Disables IPv6 protocol for management interfaces of all devices in the enclosure.

⚠️ **CAUTION:** If you disable IPv6 in an IPv6-only environment, you will lose your connection to the Onboard Administrator GUI and any SSH sessions. To reestablish your connection, you must perform the initial enclosure configuration via IPv4 networking, the Insight Display, or the Onboard Administrator serial console interface. When disabling IPv6, all connections that depend on the IPv6 protocol are closed.

**NOTE:** After disabling IPv6 to convert to an IPv4-only environment, if the location of the firmware ISO image used for EFM purposes is a USB key or an IPv6-based URL for the web server, you must use the `SET FIRMWARE MANAGEMENT URL (on page 158)` command to reenter the location of the USB or to specify an IPv4-based address for the web server. If this is not done, EFM cannot access the ISO image.

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  None

### DISABLE IPV6DYNDNS

- **Command:**
  DISABLE IPV6DYNDNS [<bay number> | ACTIVE | STANDBY]

- **Description:**
  - Disables Dynamic DNS using IPv6 for the specified bay, the Active Onboard Administrator, or the Standby Onboard Administrator.
  - If you do not specify the Onboard Administrator (<bay number>, ACTIVE, or STANDBY), the command defaults to the current (local) Onboard Administrator.
  - Disabling Dynamic DNS on the Onboard Administrator stops the Onboard Administrator’s updates to the DNS server. However, note that some DHCP servers may have a provision to update DNS...
servers directly. To completely disable Dynamic DNS updates, disable Dynamic DNS both at the Onboard Administrator as well as at the DHCP server.

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  None

### DISABLE LOGIN_BANNER

- **Command:**
  DISABLE LOGIN_BANNER

- **Description:**
  Disables the login banner from appearing when the user attempts to log in to Onboard Administrator.

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  None

### DISABLE NTP

- **Command:**
  DISABLE NTP

- **Description:**
  Disables the synchronizing of time and date with a remote server using the NTP protocol. Does not clear any NTP servers that have been configured.

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  None

### DISABLE ROUTER ADVERTISEMENTS

- **Command:**
  DISABLE ROUTER ADVERTISEMENTS

- **Description:**
  Blocks IPv6 router advertisements sent from the external management network, preventing them from entering the internal enclosure management network.

- **Access level/Bay level:**
OA administrator, OA operator

- **Restrictions:**
  - If IPv6 is disabled, this command has no effect.
  - If router advertisements are disabled, SLAAC address configuration is prevented.

  **NOTE:** When IPv6 router advertisements are disabled, the respective SLAAC addresses of the iLOs in the enclosure are retained until these addresses expire automatically based on their respective configurations. A manual reset of the iLO releases these addresses immediately.

### DISABLE SECURESH

- **Command:**
  
  DISABLE SECURESH

- **Description:**
  Disables SSH access to the Onboard Administrator.

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  None

### DISABLE SLAAC

- **Command:**
  
  DISABLE SLAAC

- **Description:**
  Disables auto-configuration of IPv6 addresses from SLAAC messages for management interfaces of all devices in the enclosure.

  **NOTE:** When SLAAC is disabled, the respective IPv6 addresses of the iLOs in the enclosure are retained until these addresses expire automatically based on their respective configurations. A manual reset of the iLO releases these addresses immediately.

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  None

### DISABLE SNMP

- **Command:**
  
  DISABLE SNMP

- **Description:**
  Disables SNMP support for the Onboard Administrator.
Does not clear the SNMP trap receivers that have been configured.
SNMP trap receivers can still be added and removed.
If you disable SNMP, then Insight Manager Agents do not work properly.

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  This operation is not allowed in FIPS Mode ON/DEBUG.

### DISABLE SSL CIPHER

- **Command:**
  
  DISABLE SSL CIPHER "<list>"

- **Description:**
  - Disables the specified security ciphers used by the Onboard Administrator for negotiating TLS connections.

  **CAUTION:** Disabling one or more ciphers might cause some clients to lose connectivity to the Onboard Administrator GUI, depending on the order and list of ciphers supported by the client.

  - Specify one or more security ciphers in double quotes and separated by commas, colons, or spaces. For example:
    "TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA"
  - To display the current status of ciphers, use **SHOW SSL CIPHER** (on page 119).

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  - Security ciphers can be disabled only in FIPS Mode ON/DEBUG. To display current FIPS Mode settings, use **SHOW FIPS MODE** (on page 112). To change FIPS Mode settings, use **SET FIPS MODE** (on page 104).
  - You cannot disable all ciphers; at least one cipher must be enabled at all times.
  - After disabling security ciphers, the Onboard Administrator web service restarts. Users using the Onboard Administrator GUI might have to sign in to the Onboard Administrator again.

### DISABLE SSL PROTOCOL

- **Command:**
  
  DISABLE SSL PROTOCOL "<list>"

- **Description:**
  - Disables the specified security protocols used by the Onboard Administrator for negotiating TLS connections.
  - Specify one or more security protocols in double quotes and separated by commas, colons, or spaces. For example:
    "TLSv1, TLSv1.1"
To display the current status of protocols and ciphers, use **SHOW SSL PROTOCOL (on page 120)**.

**Access level/Bay level:**
OA administrator

**Restrictions:**
- Security protocols can be disabled only in FIPS Mode ON/DEBUG. To display current FIPS Mode settings, use **SHOW FIPS MODE (on page 112)**. To change FIPS Mode settings, use **SET FIPS MODE (on page 104)**.
- You cannot disable all protocols; at least one protocol must be enabled at all times.
- After disabling security protocols, the Onboard Administrator web service restarts. Users using the Onboard Administrator GUI might have to sign in to the Onboard Administrator again.

### DISABLE TELNET

**Command:**
DISABLE TELNET

**Description:**
Disables telnet access to the Onboard Administrator

**Access level/Bay level:**
OA administrator, OA operator

**Restrictions:**
None

### DISABLE TRUSTED HOST

**Command:**
DISABLE TRUSTED HOST

**Description:**
Disables the host-based access to the Onboard Administrator. Disabling trusted hosts allows all hosts to connect to the Onboard Administrator.

**Access level/Bay level:**
OA administrator

**Restrictions:**
None

### DISABLE XMLREPLY

**Command:**
DISABLE XMLREPLY

**Description:**
Disables XML reply data return over the HTTP port
• **Access level/Bay level:**
  OA administrator, OA operator

• **Restrictions:**
  None

### DOWNLOAD CONFIG

• **Command:**
  `DOWNLOAD CONFIG <url>`

• **Description:**
  - Downloads a previously saved configuration script file from a specific IP host, and then executes it.
  - Supported protocols are HTTP, FTP, TFTP, and USB.
  - Format the `<URL>` as `protocol://host/path/file`.
  - The URL syntax for IPv4 addresses is `protocol://<ipv4 address>/path/file`.
  - The URL syntax for IPv6 addresses is `protocol://[<ipv6 address>]/path/file`.
  - If your FTP server does not support anonymous connections, you can specify a user name and password in the format `ftp://username:password@host/path/file`.

• **Access level/Bay level:**
  OA administrator

• **Restrictions:**
  - The file cannot change the Administrator account password.
  - The user password is not saved or restored by the `DOWNLOAD CONFIG` command.

### DOWNLOAD SSHKEY

• **Command:**
  `DOWNLOAD SSHKEY <url>`

• **Description:**
  - Downloads an authorized key file to use for SSH logins. The file contains the public keys for users.
  - Supported protocols are HTTP, FTP, and TFTP.
  - Format `<url>` as `protocol://host/path/file`.
  - The URL syntax for IPv4 addresses is `protocol://<ipv4 address>/path/file`.
  - The URL syntax for IPv6 addresses is `protocol://[<ipv6 address>]/path/file`.
  - If your FTP server does not support anonymous connections, you can specify a user name and password in the format `ftp://username:password@host/path/file`.

• **Access level/Bay level:**
  OA administrator

• **Restrictions:**
When the Onboard Administrator is operating in FIPS Mode, certificates must have a minimum RSA key length of 2048 bits, and the signature hash algorithm must be SHA1, SHA-224, SHA-256, SHA-384, or SHA-512.

**ENABLE ALERTMAIL**

- **Command:**
  ENABLE ALERTMAIL

- **Description:**
  Enables the sending of alert emails when an event occurs

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  You can only issue this command if the configuration has been set up.

**ENABLE DHCPV6**

- **Command:**
  ENABLE DHCPV6

- **Description:**
  Enables the active (and standby, if configured) Onboard Administrator to request a DHCPv6 IP address. Allows DHCPv6 traffic on the enclosure management network. When this mode is enabled, all IPv6 and DNS addresses are obtained from the DHCPv6 Server. If IPv6 is enabled, the ENABLE DHCPV6 setting takes effect immediately. To enable IPv6, use ENABLE IPV6 (on page 95).

  **NOTE:** For DHCPv6 addresses to be successfully configured, the ENABLE DHCPV6 setting must be enabled on the enclosure and a DHCPv6 server configured on the management network. iLOs and interconnects must be configured separately to request a DHCPv6 address. If they are configured to request DHCPv6 addresses, the ENABLE DHCPV6 and ENABLE IPV6 settings must be enabled to allow the necessary traffic on the enclosure management network.

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  For the ENABLE DHCPV6 setting to take effect, IPv6 must be enabled.

**ENABLE ENCLOSURE_ILO_FEDERATION_SUPPORT**

- **Command:**
  ENABLE ENCLOSURE_ILO_FEDERATION_SUPPORT

- **Description:**
  Enables the Onboard Administrator support required to allow peer-to-peer network communication necessary for iLO Federation among suitably capable iLOs within the enclosure.
**IMPORTANT:** Enable Enclosure iLO Federation Support only enables Onboard Administrator support to allow the peer-to-peer network communication necessary for iLO Federation among iLOs within the enclosure. To fully enable iLO Federation, each iLO must have the appropriate firmware and be configured to participate in iLO Federation. For more information, see the HP iLO 4 User Guide at the HP website (http://www.hp.com/go/ilo/docs).

- **Access level/Bay level:**
  OA administrator, OA operator
- **Restrictions:**
  None

### ENABLE ENCLOSURE_IP_MODE

- **Command:**
  ENABLE ENCLOSURE_IP_MODE
- **Description:**
  Enables Enclosure IP Mode
- **Access level/Bay level:**
  OA administrator, Operator
- **Restrictions:**
  - When using enclosure IP mode only replace the standby OA module while the enclosure is powered on to ensure persistence of Enclosure IP Mode settings.
  - You cannot ENABLE ENCLOSURE_IP_MODE in FIPS Mode ON/DEBUG.

### ENABLE FQDN_LINK_SUPPORT

- **Command:**
  ENABLE FQDN_LINK_SUPPORT
- **Description:**
  Enables the Onboard Administrator to display an FQDN-based web address link in addition to the usual IP-based web address links used for accessing an iLO or interconnect from the Onboard Administrator GUI. The Onboard Administrator queries a DNS server that performs a reverse lookup for the FQDN of the device and generates the FQDN-based web address (formatted as host-name.domain-name.com).

  When the FQDN setting is enabled, the lists of URL links for all the appropriate devices (iLOs and interconnects) are automatically refreshed and updated with the corresponding FQDNs.

  FQDN link support is useful in IPv6-based remote access environments that depend on an IPv4-based enclosure management network with IPv4 DNS. It is not meant for pure IPv6 environments with IPv6 DNS.

- **Access level/Bay level:**
  OA administrator, OA operator
- **Restrictions:**
- An IPv4 DNS server must be configured on the Onboard Administrator, and the devices to be accessed must be registered for reverse lookup with the DNS name server.
- A DNS IP address must be configured on the Onboard Administrator. Use ADD OA DNS (on page 77).

**ENABLE HTTPS**

- **Command:**
  ENABLE HTTPS
- **Description:**
  Enables HTTPS access to the Onboard Administrator
- **Access level/Bay level:**
  OA administrator, OA operator
- **Restrictions:**
  None

**ENABLE IPV6**

- **Command:**
  ENABLE IPV6
- **Description:**
  Enables IPv6 protocol for management interfaces of all devices in the enclosure.
- **Access level/Bay level:**
  OA administrator, OA operator
- **Restrictions:**
  None

**ENABLE IPV6DYNDNS**

- **Command:**
  ENABLE IPV6DYNDNS [<bay number> | ACTIVE | STANDBY]
- **Description:**
  - Enables Dynamic DNS using IPv6 for either the specified bay, the Active Onboard Administrator, or the Standby Onboard Administrator.
  - If you do not specify the Onboard Administrator (<bay number>, ACTIVE, or STANDBY), the command defaults to the current (local) Onboard Administrator.
  - DDNS allows you to use a host name for the Onboard Administrator. The host name is registered with a DNS server. DDNS (DDNS) updates the DNS server with new or changed records for IP addresses. This allows you to use the same host name over time, although the dynamically assigned IP address might change.
- **Access level/Bay level:**
OA administrator, OA operator

- **Restrictions:**
  IPv6 Dynamic DNS requires that a valid DNS server (either IPv4 or IPv6) be configured on the Onboard Administrator.

### ENABLE LOGIN_BANNER

- **Command:**
  `ENABLE LOGIN_BANNER`

- **Description:**
  Enables the display of the configured login banner when the user attempts to log in to the Onboard Administrator.

- **Access level /Bay level:**
  OA administrator

- **Restrictions:**
  None

### ENABLE NTP

- **Command:**
  `ENABLE NTP`

- **Description:**
  Enables NTP support for the Onboard Administrator

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  None

### ENABLE ROUTER ADVERTISEMENTS

- **Command:**
  `ENABLE ROUTER ADVERTISEMENTS`

- **Description:**
  Allows router advertisements from the external management network onto the internal enclosure management network.

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  If IPv6 is disabled, this command has no effect.
ENABLE SECURESSH

- **Command:**
  
  ENABLE SECURESSH

- **Description:**
  Enables SSH support for the Onboard Administrator

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  None

ENABLE SLAAC

- **Command:**
  
  ENABLE SLAAC

- **Description:**
  Enables auto-configuration of IPv6 addresses from SLAAC messages for management interfaces of all devices in the enclosure.

**NOTE:** For SLAAC addresses to be successfully configured, the ENABLE SLAAC and ENABLE ROUTER ADVERTISEMENTS settings must be enabled on the enclosure. In addition, an IPv6 router must be configured on the enclosure management network to provide the SLAAC addresses via Router Advertisements. iLOs may need to be configured separately to obtain SLAAC addresses. To allow the necessary traffic on the enclosure management network, the ENABLE SLAAC, ENABLE IPV6, and ENABLE ROUTER ADVERTISEMENTS settings must be enabled.

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  Refer to the preceding note.

ENABLE SNMP

- **Command:**
  
  ENABLE SNMP

- **Description:**
  Enables SNMP Trap support for the Onboard Administrator

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  None
ENABLE SSL CIPHER

- **Command:**
  
  ENABLE SSL CIPHER{"<list>" | ALL}

- **Description:**
  
  o Enables the specified security ciphers used by the Onboard Administrator for negotiating TLS connections.
  
  o Specify one or more supported security ciphers in double quotes and separated by commas, colons, or spaces. For example:
    
    "TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA"
  
  o To enable all supported ciphers, specify ALL.
  
  o To display the current status of ciphers, use SHOW SSL CIPHER (on page 119).
  
  o After enabling security ciphers, the Onboard Administrator web service restarts. Users using the Onboard Administrator GUI might have to sign in to the Onboard Administrator again.

- **Access level/Bay level:**
  
  OA administrator

- **Restrictions:**
  
  o Security ciphers can be enabled only in FIPS Mode ON/DEBUG. To display current FIPS Mode settings, use the SHOW FIPS MODE (on page 112) command. To change FIPS Mode settings, use the SET FIPS MODE (on page 104) command.

ENABLE SSL PROTOCOL

- **Command:**
  
  ENABLE SSL PROTOCOL{"<list>" | ALL}

- **Description:**
  
  o Enables the specified security protocols used by the Onboard Administrator for negotiating TLS connections.
  
  o Specify one or more supported security protocols in double quotes and separated by commas, colons, or spaces. For example:
    
    "TLSv1, TLSv1.1, TLSv1.2"
  
  o To enable all supported protocols or ciphers, specify ALL.
  
  o To display the current status of protocols and ciphers, use SHOW SSL PROTOCOL (on page 120).
  
  o After enabling security protocols, the Onboard Administrator web service restarts. Users using the Onboard Administrator GUI might have to sign in to the Onboard Administrator again.

- **Access level/Bay level:**
  
  OA administrator

- **Restrictions:**
  
  o Security protocols can be enabled only in FIPS Mode ON/DEBUG. To display current FIPS Mode settings, use SHOW FIPS MODE (on page 112). To change FIPS Mode settings, use SET FIPS MODE (on page 104).
ENABLE TELNET

- **Command:**
  ENABLE TELNET

- **Description:**
  Enables telnet access to the Onboard Administrator

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  You cannot enable TELNET in FIPS Mode ON/DEBUG.

ENABLE TRUSTED HOST

- **Command:**
  ENABLE TRUSTED HOST

- **Description:**
  Enables IP security for the Onboard Administrator

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  None

ENABLE XMLREPLY

- **Command:**
  ENABLE XMLREPLY

- **Description:**
  Enables XML reply data over an HTTP connection

- **Access Level/Bay Level:**
  OA administrator, OA operator

- **Restrictions:**
  None

REMOVE OA ADDRESS IPV6

- **Command:**
  REMOVE OA ADDRESS IPV6 {<bay number>} <ipv6 address/prefix length>

- **Description:**
Enclosure network configuration commands

Removes the IPv6 static address for the Onboard Administrator. If IPv6 is enabled, then this command takes effect immediately. If no Onboard Administrator number is provided, the command defaults to the active Onboard Administrator.

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  - The prefix length is mandatory.
  - The `<ip address>` value must be in the form `####:####:####:####:####:####:####:####/###`, where each `####` ranges from 0 to FFFF. A compressed version of the same IPv6 address is also supported. The prefix `/###` ranges from 1 to 128.

### REMOVE OA DNS

- **Command:**
  
  REMOVE OA DNS [<OA bay number>] <ip address>

- **Description:**
  Removes the IP address of a DNS server from the list for the specified Onboard Administrator. The DNS servers are used only if the system is configured to use a static IP address. If no bay number is provided, the command defaults to the active Onboard Administrator.

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  The `<ip address>` must be in the form `###.###.###.###`, where each `###` ranges from 0 to 255.

### REMOVE OA DNS IPV6

- **Command:**
  
  REMOVE OA DNS IPV6 {<OA bay number>} <ipv6 address{/prefix length}>

- **Description:**
  Removes the specified DNS IPv6 address from the list of DNS addresses for the specified Onboard Administrator. If a bay number is not specified, then the command defaults to the active Onboard Administrator.

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  - A maximum of two DNS servers can be added.
  - The `<ip address>` must be in the form `####:####:####:####:####:####:####:####` or `####:####:####:####:####:####:####:####/###` (with a prefix), where each `####` ranges from 0 to FFFF and the prefix `/###` ranges from 1 to 128.
REMOVE OA ROUTE IPV6

- **Command:**
  
  ```
  REMOVE OA ROUTE IPV6 [<bay number> | ACTIVE | STANDBY] {ALL | <route destination> [<route gateway>]}
  ```

- **Description:**
  
  - Removes an IPv6 static route from the Onboard Administrator IPv6 routing table.
  - If you do not specify the Onboard Administrator (`<bay number>`, ACTIVE, or STANDBY), the command defaults to the current (local) Onboard Administrator.
  - The `<route destination>` specifies the IPv6 address of the static route, while the `<route gateway>` specifies the IPv6 address of the gateway using this static route. To remove all IPv6 routes, specify ALL.

  **CAUTION:** Adding or removing a static route might close client connections to the Onboard Administrator.

- **Access level/Bay level:**
  
  OA administrator, OA operator

- **Restrictions:**
  
  - The `<route destination>` IPv6 address must be in the form `####:####:####:####:####:####:####:####/###` (with a prefix), where each `####` ranges from 0 to FFFF. A compressed version of the same IPv6 address is also supported. The prefix `/###` ranges from 1 to 128. A compressed version of the same IPv6 address is also supported.
  - If specified, the `<route gateway>` IPv6 address must be in the form `####:####:####:####:####:####:####:####` where `####` ranges from 0 to FFFF. Do not specify a prefix. A compressed version of the same IPv6 address is also supported.
  - The gateway must be reachable from both the Onboard Administrator network and the external network.

REMOVE SNMP TRAPRECEIVER

- **Command:**
  
  ```
  REMOVE SNMP TRAPRECEIVER <host> {"<community name>"}
  ```

- **Description:**
  
  - Removes an IP address from the list of systems that receive SNMP traps. If the same IP address is listed multiple times with different communities, all instances of the IP address disappear unless `<community>` specifies which one is to be removed.
  - Removes an existing trap receiver from the SNMP configuration. If the same `<host>` is listed multiple times with different communities, all instances of the `<host>` disappears unless `<community name>` specifies which one is to be removed.
  - The `<host>` value can be either an IPv4 address, an IPv6 address, or a DNS name.

- **Access level/Bay level:**
  
  OA administrator, OA operator

- **Restrictions:**
IPv6 addresses cannot specify the network prefix length.

**REMOVE SNMP TRAPRECEIVER V3**

- **Command:**
  
  `REMOVE SNMP TRAPRECEIVER V3 {<host> [<user name>]}`

- **Description:**
  
  - Removes an existing trap receiver address from the SNMP configuration.
  - This command is an extension of the existing `REMOVE SNMP TRAPRECEIVER` command. If a user name is specified, all traps matching the host/user name combination are removed. If no user name is specified, all traps matching the host name are removed.

- **Access level/Bay level:**
  
  OA administrator, OA operator

- **Restrictions:**
  
  - The `<host>` value can be an IPv4 address, an IPv6 address, or a DNS name (maximum of 64 characters).
  - IPv6 addresses must be typed without the network prefix length.

**REMOVE SNMP USER**

- **Command:**
  
  `REMOVE SNMP USER "<username>" [ENGINEID "<engineid>"]`

- **Description:**
  
  Deletes the user specified by the `username` parameter. If the `engineid` parameter is not set, all users with matching `username` are deleted. Otherwise, users matching the `username` and `engine id` pair are deleted.
  
  All traps/informs associated with this user are also deleted.

- **Access level/Bay level:**
  
  OA administrator

- **Restrictions:**
  
  The `engine id` parameter must be a series of hexadecimal characters up to 32 bytes or 64 characters in length. The `engine id` can be prefixed with "0x."

**REMOVE TRUSTED HOST**

- **Command:**
  
  `REMOVE TRUSTED HOST <ip address>`

- **Description:**
  
  Removes an IPv4 or IPv6 address from the list of addresses being handled by the IP Security feature.
CAUTION: When using the Trusted Hosts feature in an environment with multiple enclosures connected via enclosure link cables, ensure that all linked enclosures have the same Trusted Hosts settings. Linked enclosures that do not have the same Trusted Hosts settings may allow a web GUI user to access a protected enclosure from a non-trusted client.

- **Access level/Bay level:**
  OA administrator
- **Restrictions:**
  None

**SET ALERTMAIL MAILBOX**

- **Command:**
  ```
  SET ALERTMAIL MAILBOX "<email address>"
  ```
- **Description:**
  Sets the email address where events are sent
- **Access level/Bay level:**
  OA administrator, OA operator
- **Restrictions:**
  None

**SET ALERTMAIL SENDERDOMAIN**

- **Command:**
  ```
  SET ALERTMAIL SENDERDOMAIN "<domain>"
  ```
- **Description:**
  Sets the AlertMail domain. This command is the DNS domain where the Onboard Administrator is located (for example, http://www.AB.com).
- **Access level/Bay level:**
  OA administrator, OA operator
- **Restrictions:**
  The OA accepts domain name character strings subject to the following constraints:
  - The string must be between 1 and 255 characters in length.
  - The characters are case insensitive.
  - The first character of the domain name must be alphanumeric, while the last character can be either alphanumeric or a period.
  - The characters between the first and last character can be alphanumeric, dash or period.
  - If one or more periods appear in the name, they are used to delimit labels.
  - Labels are between 1 and 63 characters long and begin and end with an alphanumeric character.
  - The last label is referred as the top-level domain and cannot consist of all numeric characters.
SET ALERTMAIL SENDERNAME

- **Command:**
  SET ALERTMAIL SENDERNAME "<name>"

- **Description:**
  Sets the AlertMail sender’s name. This name is attached to the email address in the from field in an alertmail message.

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  - The <name> value may contain alphanumeric, dash(-), underscore(_), and space characters.
  - Maximum length is 40 characters.

SET ALERTMAIL SMTPSERVER

- **Command:**
  SET ALERTMAIL SMTPSERVER [ <host> ]

- **Description:**
  Sets the SMTP server. This is the mail server where the Onboard Administrator delivers its e-mail based events.
  The <host> value can be either an IPv4 address, an IPv6 address, or a DNS name.

- **Access level/Bay level:**
  Administrator, OA operator

- **Restrictions:**
  IPv6 addresses cannot specify the network prefix length.

SET FIPS MODE

- **Command:**
  SET FIPS MODE {ON ["<password>"], DEBUG ["<password>"], OFF ["<password>"],}

- **Description:**
  - Sets FIPS Mode ON, DEBUG, or OFF. FIPS Mode ON enforces use of the Onboard Administrator in a FIPS 140-2-compliant mode, using only approved cryptographic protocols and ciphers.
  - FIPS Mode DEBUG sets the Onboard Administrator to an environment similar to FIPS Mode ON. FIPS Mode DEBUG has the functionality of FIPS Mode ON but is not considered FIPS-compliant.
  - If you do not provide the password when changing the FIPS Mode setting, you are prompted for the password. In script mode, the password is mandatory. In FIPS Mode ON/DEBUG, ensure that a strong password is set.
  - When changing the FIPS Mode setting, strong passwords are enabled, minimum password length is set to eight characters, and a new Administrator account password is requested.
o With FIPS Mode ON/DEBUG, the Enclosure IP mode, Telnet, SNMPv1, and SNMPv2 protocols are
disabled, while SNMPv3 is available.
o The Onboard Administrator restarts after all changes are made.
o Any change to the FIPS Mode setting performs a Restore to Factory Default operation. All existing
settings are lost.
o Protocol and cipher selections may be modified using ENABLE SSL and DISABLE SSL.

• **Access level/Bay level:**
  OA administrator

• **Restrictions:**
  o When the Onboard Administrator is operating in FIPS Mode, certificates must have a minimum RSA
  key length of 2048 bits, and the signature hash algorithm must be SHA1, SHA-224, SHA-256,
  SHA-384, or SHA-512.
  Certificates are used in various features such as the following:
  — Onboard Administrator certificate signing requests — for more information, see the command
    GENERATE CERTIFICATE (on page 53)
  — LDAP — for more information, see "Directory commands (on page 40)"
  — Two-Factor Authentication — for more information, see "Two-Factor Authentication commands
    (on page 35)"
  — Insight Remote Support — for more information, see "HP Insight Remote Support commands (on
    page 213)"
  — HP SIM Single Sign-On — for more information, see "HP SIM commands (on page 49)"

**SET HTTP REQUESTREADTIMEOUT**

• **Command:**

  SET HTTP REQUESTREADTIMEOUT {HEADER <min> {- <max>} {MINRATE <rate>}} | {BODY
  <min> {- <max> {MINRATE <rate>}} | NONE}

• **Description:**
  o Sets timeout and byte-transfer rate parameters to control HTTP client requests sent to the Onboard
  Administrator GUI web server. This feature can help mitigate denial-of-service attacks whereby a
  malicious client opens many TCP connections to tie up all available connections, then slowly writes
  a few bytes at a time to prevent legitimate clients from accessing the Onboard Administrator. The
  timeout values can restrict the length of time the attacking client can keep the connection open. If the
  client fails to send the header or body within the respective configured timeouts, a 408 REQUEST
  TIME OUT error is sent.
  o The <min> (minimum) and <max> (maximum) values specify the number of seconds. The <rate>
  value specifies the bytes per second.
  o If you specify the <min> value without a <max> value, the entire header or body must be received
  within <min> seconds.
  o If a <max> value is provided, then the timeout will be extended in one-second intervals from <min>
  to <max> as long as <rate> bytes are received each second.
  o The HEADER and BODY keywords, with their respective parameters, may be specified in either
  order.
- `MINRATE` is optional unless `<max>` is specified.
- To clear the setting and disable the feature, specify `NONE` (the default).

⚠️ **CAUTION:** Configure this setting with care. An inappropriate setting can result in client connectivity issues. To avoid such issues, tune the setting for the specifics of your network operating environment and validate this setting in a non-production environment prior to applying it to your production environment. For mitigating denial of service attacks, recommended settings are:

```plaintext
SET HTTP REQUESTREADTIMEOUT HEADER 3-8 MINRATE 500 BODY 5-10 MINRATE 500
```

For more information, see the latest Apache documentation for the `RequestReadTimeout` directive.

- **Access level/Bay level:**
  OA administrator, OA operator
- **Restrictions:**
  - Values for all parameters must be positive.
  - At least one `<min>` must be specified.
  - The `<max>` value must be greater than the corresponding `<min>` value.

---

**SET IPCONFIG**

- **Command:**
  ```plaintext
  SET IPCONFIG {DHCP | STATIC} [<OA bay number>] [DYNAMICDNS] <ip address> <netmask> [<gateway> [<DNS1 address> [<DNS2 address>]]]
  ```

- **Description:**
  - Configures the OA to IPv4 static mode or DHCP mode.
  - In **STATIC** mode, the IP address and netmask are set to the specified `<ip address>` and `<netmask>` respectively. These settings take effect immediately. If the gateway address and/or DNS addresses are not specified, they are cleared. The gateway and DNS address can also be set by using the `SET OA GATEWAY` and `ADD OA DNS` commands. The command syntax for setting static mode is as follows:
    ```plaintext
    SET IPCONFIG STATIC [<OA bay number>] <ip address> <netmask> [<gateway> [<DNS1 address> [<DNS2 address>]]]
    ```
  - In **DHCP** mode, the IP address, netmask, gateway address, and DNS addresses are obtained from the DHCP. This setting immediately takes effect. If `DYNAMICDNS` is specified, then the DNS server is notified of the new IP address of the system when received from the DHCP server. The command syntax for setting DHCP mode is as follows:
    ```plaintext
    SET IPCONFIG DHCP [<OA bay number>] [DYNAMICDNS]
    ```

⚠️ **CAUTION:** When enabling DHCP for IPv4, any static IPv4 settings are lost.

- **Access level/Bay level:**
  OA administrator, OA operator
- **Restrictions:**
  None
SET LOGIN_BANNER_TEXT

- **Command:**
  
  SET LOGIN_BANNER_TEXT <end marker> <\n> <banner text> <\n> <end marker>

- **Description:**
  
  Sets the login banner text to be displayed when the user attempts to log in to the Onboard Administrator.

  To enter the login banner text:

  a. Start with a string that does not appear within the certificate (the end marker).
  b. Insert a newline character by pressing **Enter**.
  c. Paste the certificate on the command line.
  d. Insert a newline character by pressing **Enter**.
  e. Insert the end marker.
  f. Issue the command by pressing **Enter**.

  Failure to give a proper end marker before and after the banner text might cause the interface to wait for the appropriate end marker indefinitely.

- **Access level/Bay level:**
  
  OA administrator

- **Restrictions:**
  
  o This command is only available in script mode.
  o The minimum length of the banner text must be 1 character and the banner text cannot exceed 1500 characters. Each newline counts toward the limit. Carriage returns (if present) are stripped and do not count toward the limit.
  o The command accepts English (ASCII) characters only.
  o The characters '%' and '\' are not permitted as part of the banner text itself, but you can use them as characters in the end marker to make a unique string.
  o The end marker must not consist of all numeric characters (for example, 1245 or 85213).
  o The banner text must contain at least one visible character. Non-printable characters "%", "<", ">", "(" , ")", "#", "&", and "\" are not allowed.

SET NTP POLL

- **Command:**
  
  SET NTP POLL <seconds>

- **Description:**
  
  Sets the polling interval of the NTP servers

- **Access level/Bay level:**
  
  OA administrator, OA operator

- **Restrictions:**
  
  Poll time should be between 60 and 86,400 seconds.
SET NTP PRIMARY

- **Command:**
  
  SET NTP PRIMARY <host>

- **Description:**
  Sets the primary server used for synchronizing time and date using the NTP. The <host> value can be an IPv4 address, an IPv6 address, or a DNS name.

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  IPv6 addresses cannot specify the network prefix length.

SET NTP SECONDARY

- **Command:**
  
  SET NTP SECONDARY <host>

- **Description:**
  Sets the secondary server used for synchronizing time and date using the NTP. The <host> value can be either an IPv4 address, an IPv6 address, or a DNS name.

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  IPv6 addresses cannot specify the network prefix length.

SET OA GATEWAY

- **Command:**
  
  SET OA GATEWAY [〈bay number〉 | ACTIVE | STANDBY] <ip address>

- **Description:**
  - Sets the network default gateway for IPv4.
  - This gateway is used only if the system is configured to use a static IP address rather than the DHCP protocol.
  - If you do not specify the Onboard Administrator (〈bay number〉, ACTIVE, or STANDBY), the command defaults to the current (local) Onboard Administrator.

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  The <ip address> must be in the form ###.###.###.###, where each ### ranges from 0 to 255.
SET OA GATEWAY IPV6

- **Command:**
  SET OA GATEWAY IPV6 [<bay number> | ACTIVE | STANDBY] <ip address>

- **Description:**
  - Sets the network default gateway for IPv6.
  - This gateway is used only if the system is configured to use a static IP address rather than the DHCP protocol.
  - If you do not specify the Onboard Administrator (<bay number>, ACTIVE, or STANDBY), the command defaults to the current (local) Onboard Administrator.
  - The Onboard Administrator can accept IPv6 gateway configuration directly via the specified static IP address, and if router advertisements are configured, via router advertisements from IPv6 routers on the management network. The gateway configuration from router advertisements overrides the static IPv6 gateway setting. To determine the IPv6 gateway currently in use by the Onboard Administrator, use either SHOW NETWORK (on page 115) or SHOW OA NETWORK (on page 146).

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  The <ip address> must be in the form ####:####:####:####:####:####:####:####, where each #### ranges from 0 to FFFF. A compressed version of the same IPv6 address is also supported.

SET OA NAME

- **Command:**
  SET OA NAME [<bay number> | ACTIVE | STANDBY] "<OA name>"

- **Description:**
  - Sets the Onboard Administrator name.
  - If you do not specify the Onboard Administrator (<bay number>, ACTIVE, or STANDBY), the command defaults to the current (local) Onboard Administrator.

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  The Onboard Administrator name is 1 to 32 characters long including all alphanumeric characters and the dash (-).

SET OA UID

- **Command:**
  SET OA UID [<bay number> | ACTIVE | STANDBY] {ON | OFF}

- **Description:**
  - Sets the Onboard Administrator UID on or off.
If you do not specify the Onboard Administrator (bay number, ACTIVE, or STANDBY), the command defaults to the current (local) Onboard Administrator.

- **Access level/Bay level:**
  All
- **Restrictions:**
  None

### SET SECURESSH SERVER KEX DHG1

- **Command:**
  ```plaintext
  SET SECURESSH SERVER KEX DHG1 [ ENABLE | DISABLE ]
  ```
- **Description:**
  Enables insecure diffie-hellman-group1-sha1 key exchange on the Onboard Administrator’s SSH server.
- **Access level/Bay level:**
  OA administrator
- **Restrictions:**
  The default is disabled on Onboard Administrator 4.01; on subsequent versions, the default is enabled unless FIPS Mode is ON/DEBUG.

### SET SERIAL BAUD

- **Command:**
  ```plaintext
  SET SERIAL BAUD [ 9600 | 19200 | 38400 | 57600 | 115200 ]
  ```
- **Description:**
  Configures the baud rate settings for the OA serial console port.
- **Access level/Bay level:**
  OA administrator (only allowed from Active OA)
- **Restrictions:**
  None

### SET SNMP COMMUNITY

- **Command:**
  ```plaintext
  SET SNMP COMMUNITY {READ | WRITE} "<community name>"
  ```
- **Description:**
  Sets the community name for the read or write SNMP community. If a blank write community name is given, then SNMP set commands are disabled until a non-empty community name is given.
- **Access level/Bay level:**
OA administrator, OA operator

- **Restrictions:**
  - The write <community name> must be no more than 20 characters long, and the read <community name> must be 1 to 20 characters long.
  - All printable characters are valid.
  - The default read community name is public.
  - The default write community name is public.

**SET SNMP ENGINEID**

- **Command:**
  
  SET SNMP ENGINEID "<engineid>"

- **Description:**
  Sets the SNMPv3 engine ID for the enclosure. The final engine ID will be a hexadecimal string derived from the <engineid> value.

  Use the SHOW SNMP command to display the current engine ID.

- **Access level/Bay level:**
  
  OA administrator, OA operator

- **Restrictions:**
  - The <engineid> must be between 1 and 27 characters in length. The final engine ID will be a hexadecimal string derived from this value.
  - Any local users must be deleted and recreated after changing the local engine ID.

- **Example:**

  OA> set snmp engineid testid

  SNMP engine id set to "0x8000000b04746573746964"

**SET SNMP CONTACT**

- **Command:**
  
  SET SNMP CONTACT "<contact>"

- **Description:**
  Configures the name of the system contact. The default contact is blank.

- **Access level/Bay level:**
  
  OA administrator, OA operator

- **Restrictions:**
  - The <contact> must be no more than 20 characters long.
  - Any printable character is acceptable. If <contact> includes spaces or hash characters (#), include it within double quotes.
SET SNMP LOCATION

- Command:
  SET SNMP LOCATION "<location>"

- Description:
  Configures the SNMP location of the enclosure. The default location is blank.

- Access level/Bay level:
  OA administrator, OA operator

- Restrictions:
  - The <location> must be no more than 20 characters long.
  - Any printable character is acceptable. If <location> includes spaces or hash characters (#), include it within double quotes.

SHOW FIPS MODE

- Command:
  SHOW FIPS MODE

- Description:
  Displays the FIPS Mode setting.

- Access level/Bay level:
  OA administrator, OA operator, and OA user

- Restrictions:
  - In ON mode, Onboard Administrator is in a FIPS 140-2-compliant mode, using only FIPS 140-2 approved algorithms such as AES and TLSv1.2.
  - In DEBUG mode, Onboard Administrator is in a similar state as ON but with option for HP debug support.

- Example:
  OA-E4115BECFBAB> show fips mode

  FIPS Mode is Off

SHOW HEALTH

- Command:
  SHOW HEALTH

- Description:
  Displays current health of all components in the enclosure. If a component is degraded or failed, a cause and corrective action are provided.

- Access level/Bay level:
  All

- Restrictions:
### Example: Enclosure Health:

- **Enclosure Health:**
  - Enclosure: OK
  - Power Subsystem: OK
  - Cooling Subsystem: OK

### Blade Health:

<table>
<thead>
<tr>
<th>Bay Status</th>
<th>Problem</th>
<th>Corrective Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>---</td>
<td>-------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>1</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Absent</td>
<td></td>
</tr>
<tr>
<td>3a</td>
<td>Error</td>
<td>Management Processor</td>
</tr>
<tr>
<td>3b</td>
<td>OK</td>
<td>iLO Network</td>
</tr>
<tr>
<td>4</td>
<td>Absent</td>
<td></td>
</tr>
<tr>
<td>5a</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>5b</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Absent</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Absent</td>
<td></td>
</tr>
<tr>
<td>8a</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>8b</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Subsumed</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>11a</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>11b</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>12a</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>12b</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Absent</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Absent</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Absent</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Absent</td>
<td></td>
</tr>
</tbody>
</table>

### Interconnect Health:

<table>
<thead>
<tr>
<th>Bay Status</th>
<th>Problem</th>
<th>Corrective Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>---</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SHOW LOGIN_BANNER

- **Command:**
  SHOW LOGIN_BANNER

- **Description:**
  Displays the login banner settings including:
  - Login banner display on user login enabled/disabled
• Currently configured login banner text (if any)

---

**Access level / Bay level:**
OA administrator, OA operator, OA user

**Restrictions:**
None

**Example:**
OA-0018FE2757AD> show login_banner

```
Login Banner:
Status : Enabled
Login Banner Text : This is sample login banner text.
```

Do not attempt to access this system without proper authorization.

Using this system without proper authorization can result in serious penalties.

---

**SHOW NETWORK**

---

**Command:**
SHOW NETWORK

**Description:**
Displays enclosure and Onboard Administrator network settings, including:
- IPv4 information
- IPv6 information
- DHCP status
- SLAAC status
- Dynamic DNS status
- Gateway address
- Static Default Gateway
- Current Default Gateway
- IPv6 static route
- DNS addresses
- MAC address
- HTTP and HTTPS server status
- SNMP status
- SSH status
- FIPS Mode status
- Trusted Host status
- HPSIM trust mode status
- Telnet status
- AlertMail status
- NTP status
- Network link settings
- Enclosure IP mode
- GUI login status
- Active Health System status
- VLAN status
- Enclosure iLO Federation Support status
- FQDN link support status
- HTTP Request Read Timeout status

- **Access level/Bay level:**
  All

- **Restrictions:**
  VLAN ID information displays only when VLAN is enabled.

- **Example:**
  OA-E4115BECFBAB> show network

Enclosure Network Settings:

- - - - - IPv6 Information - - - - -
  IPv6: Enabled
  DHCPv6: Disabled
  Router Advertisements: Enabled
  Stateless address autoconfiguration (SLAAC): Enabled

Onboard Administrator Network Settings:

- - - - - IPv4 Information - - - - -
  DHCP: Enabled - Dynamic DNS
  IPv4 Address: 11.22.333.44
  Netmask: 255.255.252.0
  Gateway Address: 11.22.333.4
  Static IPv4 DNS 1: 11.222.333.44
  Static IPv4 DNS 2: 11.222.333.55

- - - - - IPv6 Information - - - - -
  Link-local Address: ff00::e111:5bbb:feec:fbab/64
  Static Address: Not Set
  DHCPv6 Address: (Not Set)
  Stateless address autoconfiguration (SLAAC) Addresses: (Not Set)
  Static IPv6 DNS 1: Not Set
  Static IPv6 DNS 2: Not Set
  IPv6 Dynamic DNS: Enabled
  IPv6 Static Default Gateway: (Not set)
  IPv6 Current Default Gateway: (Not set)
  IPv6 Static Route: Not Set

- - - - - General Information - - - - -
  Active IPv4 DNS Servers:
    Primary: 11.222.333.44
    Secondary: 11.222.333.55
  Active IPv6 DNS Servers:
Primary: 1001::888
Secondary: Not Set
VLAN ID: 1
MAC Address: E4:11:5B:EC:FB:AB
Network Link Settings: Link Auto-negotiation

Onboard Administrator Protocol Status:
   Web (HTTP/HTTPS): Enabled
   SNMP: Disabled
   SecureSH: Enabled
   FIPS Mode: Off
   Trusted Hosts: Disabled
   HPSIM Trust Mode: Disabled
   Telnet: Disabled
   AlertMail: Disabled
      Mailbox: Not Set
      SMTP Server: Not Set
      Sender Domain: Not Set
      Sender Name: Not Set
      Sender Email: Not Set
   XML Reply: Enabled
   NTP: Disabled
      Primary NTP server: Not Set
      Secondary NTP server: Not Set
      Server Poll-Interval: 720 seconds
   Link Loss Failover: Disabled
   Link Loss Interval: 60 seconds
   Enclosure IP Mode: Disabled
   GUI Login Detail: Enabled
   Active Health System: Enabled
   VLAN: Enabled
   Enclosure iLO Federation Support: Enabled
      Enclosure enabled iLO Federation bays: 8, 16
   Fully Qualified Domain Name (FQDN) Link Support: Enabled
   HTTP Request Read Timeout: Not Set

SHOW SNMP

• **Command:**
  SHOW SNMP

• **Description:**
  Displays the SNMP configuration, including:
  o SNMP system name
  o Location
  o Contact
  o Read community name
  o Write community name
  o Engine ID
  o List of the trap destinations

• **Access level/Bay level:**
### SHOW SNMP USER

**Command:**

SHOW SNMP USER {LIST |"<username>"}

**Description:**

Displays the current information regarding SNMPv3 users. If LIST is specified, the list of current users is displayed. If a user name is specified, information regarding that user is displayed.

**Access level/Bay level:**

All

**Restrictions:**

None

**Example:**

OA> show snmp user list

<table>
<thead>
<tr>
<th>SNMPv3 User</th>
<th>Local</th>
<th>Access</th>
<th>Security</th>
<th>EngineID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bob</td>
<td>local</td>
<td>none</td>
<td>none</td>
<td>0x8000000b044866463948746b6773726b694c534756</td>
</tr>
</tbody>
</table>

OA> show snmp user bob

User: bob
Local: yes
Access: read-only
Authentication Protocol: MD5
Privacy Protocol: DES
Minimum Security Level: auth
EngineID: 0x8000000b0466697665

### SHOW SSHFINGERPRINT

**Command:**

SHOW SSHFINGERPRINT
SHOW SSHFINGERPRINT

- **Description:**
  Displays the key fingerprint of the Onboard Administrator host public key.

- **Access level/Bay level:**
  OA administrator, OA operator, OA user

- **Restrictions:**
  None

- **Example:**
  OA-0018FE27577F> SHOW SSHFINGERPRINT

SHOW SSHKEY

- **Command:**
  SHOW SSHKEY

- **Description:**
  Displays the contents of the existing SSH authorized key files.

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  None

SHOW SSL CIPHER

- **Command:**
  SHOW SSL CIPHER

- **Description:**
  Displays the status of security ciphers used by the Onboard Administrator for negotiating TLS connections.

- **Access level/Bay level:**
  OA administrator, OA operator, and OA user

- **Restrictions:**
  None

- **Example:**
  OA-E4115BECFBAB> SHOW SSL CIPHER
  show ssl cipher
  Enabled Ciphers:
  
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
  - TLS_RSA_WITH_AES_128_GCM_SHA256
  - TLS_RSA_WITH_AES_256_GCM_SHA384
  - TLS_RSA_WITH_AES_128_CBC_SHA256
SHOW SSL PROTOCOL

- **Command:**
  SHOW SSL PROTOCOL

- **Description:**
  Displays the status of security protocols used by the Onboard Administrator for negotiating TLS connections.

- **Access level/Bay level:**
  OA administrator, OA operator, and OA user

- **Restrictions:**
  None

- **Example:**
  OA-E4115BECFBAB> SHOW SSL PROTOCOL
  
  Enabled Security Protocols:
  TLSv1
  TLSv1.1
  TLSv1.2
  Disabled Security Protocols:
  None

SHOW VCMODE

- **Command:**
  SHOW VCMODE

- **Description:**
  Displays Virtual Connect Mode settings

- **Access level/Bay level:**
  All

- **Restrictions:**
  None

- **Example:**
  OA-0018FE27577F> SHOW VCMODE
  Virtual Connect Mode: Disabled

TEST ALERTMAIL

- **Command:**
  TEST ALERTMAIL

- **Description:**
Sends a test AlertMail message to the configured email address

- **Access level/Bay level:**
  Administrator, operator

**Restrictions:**
You must have OA permission to perform this command.

**TEST SNMP**

- **Command:**
  TEST SNMP

- **Description:**
  Sends a test SNMP trap to all of the configured trap destinations

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  To use this function, you must enable SNMP.
Enclosure management commands

ADD LANGUAGE

- **Command:**
  
  ADD LANGUAGE <URL>

- **Description:**
  
  - Uploads and installs a language pack.
  - Supported protocols are HTTP, FTP, TFTP, and USB.
  - The URL should be formatted as protocol://host/path/file.
  - The URL syntax for IPv4 addresses is protocol://<ipv4 address>/path/file.
  - The URL syntax for IPv6 addresses is protocol://[<ipv6 address>]/path/file.
  - If your FTP server does not support anonymous connections, you can specify a user name and password in the format ftp://username:password@host/path/file.

- **Access level/Bay level:**
  
  OA administrator, OA operator

- **Restriction:**
  
  None

CLEAR SYSLOG

⚠️ **CAUTION:** You cannot restore this information after you delete it.

- **Command:**
  
  CLEAR SYSLOG {ENCLOSURE | OA [<bay number> | ACTIVE | STANDBY]}

- **Description:**
  
  - Clears the Onboard Administrator system log.
  - If you do not specify the Onboard Administrator (<bay number>, ACTIVE, or STANDBY), the command clears the system log of the current (local) Onboard Administrator.

- **Access level/Bay level:**
  
  OA administrator, OA operator

- **Restrictions:**
  
  None

CONNECT ENCLOSURE

- **Command:**
**CONNECT ENCLOSURE**

- **Description:**
  Connects to the OA CLI on a linked enclosure. To get a list of linked enclosure names, use the `SHOW TOPOLOGY` command.

- **Access level/Bay level:**
  All

- **Restriction:**
  None

**DISABLE DHCP_DOMAIN_NAME**

- **Command:**
  `DISABLE DHCP_DOMAIN_NAME [<bay number> | ACTIVE | STANDBY]`

- **Description:**
  - Disables the DHCP domain name, allowing the user to enter a domain name instead of the one supplied by DHCP. For more information, see `SET OA DOMAIN_NAME` (on page 132).
  - If you do not specify the Onboard Administrator (<bay number>, ACTIVE, or STANDBY), the command defaults to the current (local) Onboard Administrator.
  - If the user has previously disabled the DHCP-supplied domain name, this command causes the specified Onboard Administrator to revert to using the DHCP domain name.
  - If Dynamic DNS is enabled, then the `DISABLE DHCP_DOMAIN_NAME` command will succeed; otherwise, the command will fail with the error message: Dynamic DNS is not enabled.

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restrictions:**
  This command requires that Dynamic DNS is enabled.

**DISABLE GUI_LOGIN_DETAIL**

- **Command:**
  `DISABLE GUI_LOGIN_DETAIL`

- **Description:**
  Disables extended enclosure information available in the GUI on the login page

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restriction:**
  None

**DISABLE LLF**

- **Command:**
DISABLE LLF

- **Description:**
  Disables Link Loss Failover for Onboard Administrator Redundancy.
- **Access level/Bay level:**
  OA administrator, OA operator
- **Restrictions:**
  You must have Onboard Administrator permission to perform this command.

ENABLE DHCP_DOMAIN_NAME

- **Command:**
  ENABLE DHCP_DOMAIN_NAME [<bay number> | ACTIVE | STANDBY]
- **Description:**
  - Enables the DHCP domain name.
  - If you do not specify the Onboard Administrator (<bay number>, ACTIVE, or STANDBY), the command defaults to the current (local) Onboard Administrator.
  - If the user has previously disabled the DHCP-supplied domain name, this command causes the specified OA to revert to using the DHCP domain name.
  - If Dynamic DNS is enabled, then the ENABLE DHCP_DOMAIN_NAME command will succeed; otherwise, the command will fail with the error message: Dynamic DNS is not enabled.
- **Access level/Bay level:**
  OA administrator, OA operator
- **Restrictions:**
  This command requires that Dynamic DNS is enabled.

ENABLE GUI_LOGIN_DETAIL

- **Command:**
  ENABLE GUI_LOGIN_DETAIL
- **Description:**
  Enables extended enclosure information available in the GUI on the login page
- **Access level/Bay level:**
  OA administrator, OA operator
- **Restrictions:**
  None

ENABLE LLF

- **Command:**
  ENABLE LLF
• **Description:**
  Enables Link Loss Failover for Onboard Administrator Redundancy.

• **Access level/Bay level:**
  Operator, Administrator

• **Restrictions:**
  You must have OA permission to perform this command

**REMOVE LANGUAGE**

• **Command:**
  ```
  REMOVE LANGUAGE { <language> | <language code> }
  ```

• **Description:**
  Removes the user specified language. `<language>` is the language name. `<Language code>` is a two-letter designation for a language (EN—English, JA—Japanese, ZH—Chinese). To get a list of installed language packs, use SHOW LANGUAGES command.

• **Access level/Bay level:**
  OA administrator, OA operator

• **Restriction:**
  None

**RESET ILO**

• **Command:**
  ```
  RESET ILO {<bay number>}[FORCE]
  ```

• **Description:**
  o Resets the iLO in a bay.
  o The iLO reset is initiated first via a soft reboot request using a hardware reset mechanism. If the server blade does not support this mechanism, the iLO reset is attempted by cycling sequentially through the available network-based protocols supported by iLO (IPMI, RIBCL, JSON, SSH) until iLO successfully resets or all mechanisms have been attempted without success.
  o The optional **FORCE** parameter is relevant only to server blades that support the hardware reset mechanism. Specify **FORCE** to force a reset of the iLO, initiating a hard reboot if the iLO fails to perform a soft reboot in response to the request. The behavior of the **FORCE** option depends on the current state of the iLO:
    — If the iLO is responsive, the behavior is the same with or without the **FORCE** option: iLO performs a soft reboot and closes all active connections to the iLO.
    — If the iLO is not responsive, iLO performs a hard reboot and closes all active connections to the iLO.
  o With Gen8 and earlier generations of server blades, the RESET iLO command uses iLO firmware mechanisms. If the iLO is nonresponsive when using the command, the firmware mechanisms cannot reset the iLO.

• **Access level/Bay level:**
Administrator
Blade bay

• Restrictions:
  o The hardware reset mechanism for resetting iLO is not supported on Gen8 and earlier generations of server blades. Support for the hardware reset mechanism is tested as part of command execution. Command output displays compatibility information.
  o The \texttt{FORCE} option is not supported on Gen8 and earlier generations of server blades.
  o If a double dense blade is present, specify the blade side (such as 1A), or else the iLO will not be reset.

**RESTART OA**

• Command:
  \texttt{RESTART OA [<bay number>]}

• Description:
  Resets the Onboard Administrator module specified by \texttt{<bay number>}. If no bay number is given, then the Onboard Administrator the user is logged in to is restarted.

• Access level/Bay level:
  OA administrator, OA operator

• Restrictions:
  None

**SET DATE**

• Command:
  \texttt{SET DATE MMDDhhmm \[[CC]YY][TZ]\}}

• Description:
  Sets the date of the enclosure with the following definitions:
  o MM: Month
  o DD: Day
  o hh: Hour (24-hour time)
  o mm: Minute
  o CC: Century
  o YY: Year
  o TZ: Time zone
  If you leave the time zone variable blank, then the current time zone is left in effect.

• Access level/Bay level:
  OA administrator, OA operator

• Restrictions:
  Date and time can only be set if NTP is disabled.
MM is an integer from 01 to 12.
DD is an integer from 01 to 31.
hh is an integer from 00 to 24.
mm is an integer from 00 to 60.
For valid time zones, see "Time Zone settings (on page 228)".

SET DISPLAY EVENTS

- **Command:**
  
  \[\text{SET \ DISPLAY \ EVENTS \ \{ON \ | \ OFF\}}\]

- **Description:**
  
  - Turns on or off the displaying of events that are triggered by status changes in the system.
  - This command is specific to the CLI session. To display events for new CLI sessions, the command must be issued each time a new CLI session is initiated.
  - Events that might be displayed include the following:
    - EVENT \( (dd \ mon \ mm:ss) \): Enclosure Status Changed
    - EVENT \( (dd \ mon \ mm:ss) \): Enclosure UID Status Changed
    - EVENT \( (dd \ mon \ mm:ss) \): Enclosure Shutdown
    - EVENT \( (dd \ mon \ mm:ss) \): Enclosure Information Changed
    - EVENT \( (dd \ mon \ mm:ss) \): Enclosure Name Changed
    - EVENT \( (dd \ mon \ mm:ss) \): User Permissions Changed
    - EVENT \( (dd \ mon \ mm:ss) \): Administrator Rights Changed
    - EVENT \( (dd \ mon \ mm:ss) \): Enclosure Shutdown Pending
    - EVENT \( (dd \ mon \ mm:ss) \): Enclosure Topology Changed
    - EVENT \( (dd \ mon \ mm:ss) \): Fan Status Changed
    - EVENT \( (dd \ mon \ mm:ss) \): Fan Inserted
    - EVENT \( (dd \ mon \ mm:ss) \): Fan Removed
    - EVENT \( (dd \ mon \ mm:ss) \): Thermal Subsystem Redundancy Status Changed
    - EVENT \( (dd \ mon \ mm:ss) \): Fan at Max Percentage
    - EVENT \( (dd \ mon \ mm:ss) \): Add Fan to Bay
    - EVENT \( (dd \ mon \ mm:ss) \): Remove Fan from Bay
    - EVENT \( (dd \ mon \ mm:ss) \): Fan Over Consuming Power
    - EVENT \( (dd \ mon \ mm:ss) \): Thermal Status Changed
    - EVENT \( (dd \ mon \ mm:ss) \): Power Supply Status Changed
    - EVENT \( (dd \ mon \ mm:ss) \): Power Supply Inserted
    - EVENT \( (dd \ mon \ mm:ss) \): Power Supply Removed
    - EVENT \( (dd \ mon \ mm:ss) \): Power Supply Subsystem Redundant Status Changed
    - EVENT \( (dd \ mon \ mm:ss) \): Power Supply Subsystem Overloaded
— EVENT (dd mon mm:ss): AC Failure
— EVENT (dd mon mm:ss): Inadequate Power or Cooling
— EVENT (dd mon mm:ss): Interconnect Device Status Changed
— EVENT (dd mon mm:ss): Interconnect Device Reset
— EVENT (dd mon mm:ss): Interconnect Device UID Status Changed
— EVENT (dd mon mm:ss): Interconnect Device Inserted
— EVENT (dd mon mm:ss): Interconnect Device Removed
— EVENT (dd mon mm:ss): Interconnect Device Information Changed
— EVENT (dd mon mm:ss): Interconnect Device Health LED Status Changed
— EVENT (dd mon mm:ss): Interconnect Device Thermal Status Changed
— EVENT (dd mon mm:ss): Interconnect Device CPU Fault
— EVENT (dd mon mm:ss): Interconnect Device Power Mode Changed
— EVENT (dd mon mm:ss): Enclosure Demonstration Mode
— EVENT (dd mon mm:ss): Blade Device Status Changed
— EVENT (dd mon mm:ss): Blade Device Inserted
— EVENT (dd mon mm:ss): Blade Device Removed
— EVENT (dd mon mm:ss): Blade Device Power State Changed
— EVENT (dd mon mm:ss): Blade Device Power Management Changed
— EVENT (dd mon mm:ss): Blade Device UID Status Changed
— EVENT (dd mon mm:ss): Blade Device Shutdown
— EVENT (dd mon mm:ss): Blade Device Fault
— EVENT (dd mon mm:ss): Blade Device Thermal Status Change
— EVENT (dd mon mm:ss): Blade Device Information Changed
— EVENT (dd mon mm:ss): Blade Bay Management Processor Changed
— EVENT (dd mon mm:ss): ILO Ready
— EVENT (dd mon mm:ss): Keying Error
— EVENT (dd mon mm:ss): ILO Has IP Address
— EVENT (dd mon mm:ss): Display Changed
— EVENT (dd mon mm:ss): Button Pressed
— EVENT (dd mon mm:ss): Pin Information Changed
— EVENT (dd mon mm:ss): User Note Information Changed
— EVENT (dd mon mm:ss): Chat Requested
— EVENT (dd mon mm:ss): Chat Response Sent
— EVENT (dd mon mm:ss): LCD Display State Changed
— EVENT (dd mon mm:ss): Network Information Changed
— EVENT (dd mon mm:ss): SNMP Information Changed
— EVENT (dd mon mm:ss): System Log Cleared
Enclosure management commands

— EVENT (dd mon mm:ss): Session Cleared
— EVENT (dd mon mm:ss): Time Changed
— EVENT (dd mon mm:ss): Session Started
— EVENT (dd mon mm:ss): Blade Connected
— EVENT (dd mon mm:ss): Blade Disconnected
— EVENT (dd mon mm:ss): Switch Connected
— EVENT (dd mon mm:ss): Switch Disconnected
— EVENT (dd mon mm:ss): Blade Cleared
— EVENT (dd mon mm:ss): Switch Cleared
— EVENT (dd mon mm:ss): AlertMail Information Changed
— EVENT (dd mon mm:ss): LDAP Information Changed
— EVENT (dd mon mm:ss): EBIPA Information Changed
— EVENT (dd mon mm:ss): User Information Changed
— EVENT (dd mon mm:ss): Bay Changed
— EVENT (dd mon mm:ss): Onboard Administrator Reboot
— EVENT (dd mon mm:ss): Onboard Administrator Logoff Request
— EVENT (dd mon mm:ss): User Added
— EVENT (dd mon mm:ss): User Deleted
— EVENT (dd mon mm:ss): User Enabled
— EVENT (dd mon mm:ss): User Disabled
— EVENT (dd mon mm:ss): Flash Pending
— EVENT (dd mon mm:ss): Flash Started
— EVENT (dd mon mm:ss): Flash Progress
— EVENT (dd mon mm:ss): Flash Complete
— EVENT (dd mon mm:ss): Non-iLo EBIPA

• **Access level/Bay level:**
  All

• **Restrictions:**
  Only for bays for which you have privileges

**SET ENCLOSURE ASSET**

• **Command:**
  
  SET ENCLOSURE ASSET [TAG] "<asset tag>"

• **Description:**
  o Sets the enclosure asset tag
  o The default enclosure asset tag is blank

• **Access level/Bay level:**
OA administrator, OA operator

- **Restrictions:**
The `<asset tag>` must be 0 to 32 characters long and includes all alphanumeric, underscore (\_), and dash (-) characters.

## SET ENCLOSURE NAME

- **Command:**
  ```
  SET ENCLOSURE NAME "<enclosure name>"
  ```
- **Description:**
  - Changes the enclosure name
  - The default enclosure name is the mid-plane serial number
- **Access level/Bay level:**
  OA administrator, OA operator
- **Restrictions:**
The `<enclosure name>` must be 1 to 32 characters long and includes all alphanumeric, underscore (\_), and dash (-) characters.

## SET ENCLOSURE PART_NUMBER

- **Command:**
  ```
  SET ENCLOSURE PART_NUMBER "<part number>"
  ```
- **Description:**
  Sets the part number of the enclosure
- **Access level/Bay level:**
  OA administrator
- **Restrictions:**
  Must be 10 characters in length and the first character must be a digit. Acceptable characters are all alphanumeric and the dash (-).

## SET ENCLOSURE PDU_TYPE

- **Command:**
  ```
  SET ENCLOSURE PDU_TYPE {1|2|3|4|5|6}
  ```
- **Description:**
  Sets the enclosure PDU type to:
  - 1=Single-phase
  - 2=Three-phase
  - 3=Three-phase, international
  - 4=DC Power Input Module
- 5 = Single phase IPD
- 6 = HP HVDC/1PH AC Module

**Access level/Bay level:**
OA administrator

**Restrictions:**
- `PDU_TYPE` must be 1, 2, 3, 4, 5, or 6.

### SET ENCLOSEMENT SERIAL NUMBER

- **Command:**
  ```shell
  SET ENCLOSEMENT SERIAL_NUMBER "<serial number>"
  ```
- **Description:**
  Sets the enclosure serial number.
- **Access level/Bay level:**
  OA administrator
- **Restrictions:**
  - Must be 10 characters in length. Acceptable characters include alphanumeric, dash, and underscore.
  - Remote Support must be disabled. To disable Remote Support, use `DISABLE REMOTE_SUPPORT` (on page 216).

### SET ENCLOSEMENT UID

- **Command:**
  ```shell
  SET ENCLOSEMENT UID {ON | OFF}
  ```
- **Description:**
  Turns the UID LED of the enclosure on or off.
- **Access level/Bay level:**
  OA administrator, OA operator
- **Restrictions:**
  None

### SET LLF INTERVAL

- **Command:**
  ```shell
  SET LLF INTERVAL <seconds>
  ```
- **Description:**
  Sets the Link Loss Failover Interval.
- **Access level/Bay level:**
  OA administrator, OA operator, and OA user
**SET OA DOMAIN_NAME**

- **Command:**
  
  \[\text{SET OA DOMAIN_NAME} \ [<\text{bay number}> | \text{active} | \text{standby}] \ [\"\text{<domain-name>}\" | \text{NONE}]\]

- **Description:**
  
  - Sets the Onboard Administrator domain name for the active or standby OA.
  
  - If you do not specify the Onboard Administrator (\(<\text{bay number}>\), \text{ACTIVE}, or \text{STANDBY}), the command defaults to the current (local) Onboard Administrator.
  
  - To clear the current domain name, specify \text{NONE}.
  
  - If the DHCP domain name has been disabled, the domain name specified by this command will override the DHCP domain name. This command requires that Dynamic DNS is enabled.
  
  - The setting is not effective until Dynamic DNS is enabled on OA.
  
  - The response depends on the domain name the user provides and also the \text{domain_name_override} state:
    
    - If the name has a syntax error, an \text{Invalid Arguments} error message appears, followed by the help text for the command.
    
    - If the domain name is valid and not used currently, the following message appears: \text{OA in bay X (ACTIVE/STANDBY) set to XXX}.

- **Access level/Bay level:**
  
  OA administrator

- **Restrictions:**
  
  The OA accepts domain name character strings subject to the following constraints:
  
  - The string must be between 1 and 255 characters in length.
  
  - The characters are case insensitive.
  
  - The first character of the domain name must be alphanumeric, while the last character can be either alphanumeric or a period.
  
  - The characters between the first and last character can be alphanumeric, dash or period.
  
  - If one or more periods appear in the name, they are used to delimit labels.
  
  - Labels are between 1 and 63 characters long and begin and end with an alphanumeric character.
  
  - The last label is referred as the top-level domain and cannot consist of all numeric characters.

**SET OA USB**

- **Command:**
  
  \[\text{SET OA USB} \ \{\text{FRONT} \mid \text{BACK}\}\]
• **Description:**
  Allows the Onboard Administrator to select which USB controller to enable.
  The FRONT controller enables the internal DVD drive and the front USB connector.
  The BACK controller enables the two USB ports on the rear of the KVM Option Module.
  This command has no effect on c3000 Onboard Administrator boards that are hardware revision level 'CO' and later as displayed with `SHOW OA INFO`.

• **Access level/Bay level:**
  OA Administrator

• **Restrictions:**
  A small number of c3000 Onboard Administrator boards can use only one USB controller at a time.

**SET POWER MODE**

• **Command:**
  `SET POWER MODE {NOTREDUNDANT | REDUNDANT | POWERSUPPLY}`

• **Description:**
  o Configures redundancy settings.
  o The NOTREDUNDANT setting enables all power supplies to function without regard for redundancy.
  o The POWERSUPPLY setting enables one power supply to fail without being over committed on power.
  o The REDUNDANT setting enables half of the power supplies to fail without being over committed on power.

• **Access level/Bay level:**
  OA administrator, OA operator

• **Restrictions:**
  None

**SET POWER LIMIT**

• **Command:**
  `SET POWER LIMIT {<number> | OFF}`

• **Description:**
  Sets or removes a limit on how much input power can be consumed by the enclosure. This setting is helpful if the enclosure receives power from a PDU with a limited power rating.

• **Access level/Bay level:**
  OA administrator, OA operator

• **Restrictions:**
  None
SET POWER SAVINGS

- **Command:**
  
  SET POWER SAVINGS {ON | OFF}

- **Description:**
  
  - Turns power savings mode (Dynamic Power) on or off. Enabling power savings (specify ON) turns unneeded power supplies off. (In the Onboard Administrator GUI, you turn power savings mode on or off using the Enable Dynamic Power setting from the Power Management screen.)
  
  - The increased load on the remaining power supplies increases their efficiency, resulting in less power consumption.
  
  - The default is OFF.

- **Access level/Bay level:**
  
  OA administrator, OA operator

- **Restrictions:**
  
  Dynamic Power is supported with all c3000 power supplies. It is supported with all c7000 power supplies except those operating with low-line input voltage (nominal 100-120V AC).

SET TIMEZONE

- **Command:**
  
  SET TIMEZONE "<timezone>"

- **Description:**
  
  Sets the time zone

  See Time zone settings (on page 228) for appropriate time zones. Some that are commonly used include: CET, CST6CDT, EET, EST, EST5EDT, GB, GMT, HST, MET, MST, MST7MDT, NZ, PRC, PST8PDT, UCT, and UTC.

- **Access level/Bay level**
  
  OA administrator, OA operator

- **Restrictions:**
  
  None

SHOW CONFIG

- **Command:**
  
  SHOW CONFIG

- **Description:**
  
  - Displays the current configuration command settings that can be used for recreating the settings of the enclosure.
  
  - To suspend and resume output, use the Ctrl+S and Ctrl+Q key combinations, respectively. To quit, use Ctrl+C.
You can save the output into a file that can be run in the way a shell script is run in Linux or Unix. Run the script file to restore the saved settings on this enclosure or to configure other enclosures. Passwords for users are not included.

You can download a previously saved script file by using DOWNLOAD CONFIG (on page 92).

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  None

- **Example:**
  OA-0018FE27577F> show config
  #Script Generated by Administrator
  #Generated on: Fri May 23 12:57:12 2014

  #Set Enclosure Time
  SET TIMEZONE CST6CDT
  #DATE MMDDhhmm{{CC}YY}

  #Set Enclosure Information
  SET ENCLOSURE ASSET TAG ""
  SET ENCLOSURE NAME "Snorfmann"
  SET RACK NAME "Sulaco"

  SET POWER MODE REDUNDANT
  SET POWER SAVINGS OFF
  #Power limit must be within the range of 2700-16400 Watts AC
  SET POWER LIMIT OFF
  #Enclosure Dynamic Power Cap must be within the range of 3460-7676 Watts AC
  #Derated Circuit Capacity must be within the range of 3460-7676 Watts AC
  #Rated Circuit Capacity must be within the range of 3460-7676 Watts AC
  SET ENCLOSURE POWER_CAP OFF
  --More-- (2% of 23264 bytes)

## SHOW DATE

- **Command:**
  SHOW DATE

- **Description:**
  Displays the current date, time, and time zone of the internal clock of the enclosure

- **Access level/Bay level:**
  All

- **Restrictions:**
  None

- **Example:**
  OA-0018FE27577F> SHOW DATE
  Date: 2008-04-15T10:36:46-05:00 Time Zone: CST6CDT
SHOW DISPLAY EVENTS

- **Command:**
  
  SHOW DISPLAY EVENTS

- **Description:**
  Displays whether event notification is on or off

- **Access level/Bay level:**
  All

- **Restrictions:**
  None

- **Example:**
  OA-0018FE27577F> SHOW DISPLAY EVENTS
  Display Events is set to OFF.

SHOW ENCLOSURE FAN

- **Command:**
  
  SHOW ENCLOSURE FAN {<fan number> | ALL}

- **Description:**
  Displays information about, and current status of the specified enclosure fan

- **Access level/Bay level:**
  All

- **Restrictions:**
  None

- **Example:**
  OA-0018FE27577F> show enclosure fan 1
  Fan #1 information:
  Status: OK
  Speed: 48 percent of Maximum speed
  Maximum speed: 18000
  Minimum speed: 10
  Power consumed: 21
  Product Name: Active Cool 200 Fan
  Part Number: 412140-B21
  Spare Part Number: 413996-001
  Version: 2.7
  Diagnostic Status:
  Internal Data OK
  Location OK
  Device Failure OK
  Device Degraded OK
  Missing Device OK

SHOW ENCLOSURE INFO

- **Command:**
SHOW ENCLOSURE INFO

- **Description:**
  Displays:
  - Enclosure name
  - Enclosure type
  - Onboard Administrator hardware version
  - Enclosure Rack U Position
  - Enclosure part number
  - Serial number
  - Asset tag
  - Onboard Administrator MAC address

- **Access level/Bay level:**
  All

- **Restrictions:**
  None

- **Example:**
  OA-0018FE2F6941> show enclosure info
  Enclosure Information:
  Enclosure Name: USE818AMMP
  Enclosure Type: BladeSystem c7000 Enclosure
  Enclosure Rack U Position: 6
  Part Number: 412152-B21
  Serial Number: USE818AMMP
  UUID: 09USE818AMMP
  Asset Tag:
  Midplane Spare Part Number: 414050-001
  Solutions ID: 0000000000000000
  Power Distribution Unit:
    PDU Type: HP AC Module, Single Phase
    PDU Spare Part Number: 413494-001
  Onboard Administrator Tray Information:
    Type: HP BladeSystem c7000 Onboard Administrator Tray
    Spare Part Number: 416000-001
    Serial Number: OI84MP1625

SHOW ENCLOSURE LCD

- **Command:**
  SHOW ENCLOSURE LCD

- **Description:**
  Displays information about the Insight Display screen

- **Access level/Bay level:**
  All

- **Restrictions:**
  None
SHOW ENCLOSURE POWER_SUMMARY

- **Command:**
  SHOW ENCLOSURE POWER_SUMMARY

- **Description:**
  Displays a detailed summary of the enclosure's present power state.

- **Access level/Bay level:**
  OA Administrator

- **Restrictions:**
  Administrator account privileges are required.

- **Example:**
  OA-0018FE27577F> show enclosure power_summary

Enclosure Bay Output Allocation:

<table>
<thead>
<tr>
<th>Bay</th>
<th>Power Allocated (Watts DC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devices</td>
<td>1314</td>
</tr>
<tr>
<td>Interconnects</td>
<td>+ 25</td>
</tr>
<tr>
<td>Fans</td>
<td>+ 480</td>
</tr>
<tr>
<td></td>
<td>= 1819</td>
</tr>
</tbody>
</table>

Enclosure Output Power Summary:

<table>
<thead>
<tr>
<th>Enclosure</th>
<th>Watts DC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Capacity</td>
<td>3600</td>
</tr>
<tr>
<td>Power Allocation</td>
<td>- 1819</td>
</tr>
<tr>
<td>Power Available</td>
<td>= 1781</td>
</tr>
</tbody>
</table>

Enclosure Input Power Summary:

<table>
<thead>
<tr>
<th>Enclosure</th>
<th>Watts AC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Present Power</td>
<td>822</td>
</tr>
<tr>
<td>Max Input Power</td>
<td>8500</td>
</tr>
<tr>
<td>Dynamic Power Cap</td>
<td>Not Set</td>
</tr>
<tr>
<td>Power Limit</td>
<td>8500</td>
</tr>
</tbody>
</table>

Device Bay Power Summary:

<table>
<thead>
<tr>
<th>Bay</th>
<th>Name</th>
<th>Power Allocated (Watts DC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>---</td>
<td>--------------</td>
<td></td>
</tr>
</tbody>
</table>
SHOW ENCLOSURE POWERSUPPLY

- **Command:**
  SHOW ENCLOSURE POWERSUPPLY {ALL | <power supply number> [{, | - } <power supply number>]}  

- **Description:**
  Displays:
  - Power supply status
  - AC input status
  - Capacity
  - Input voltage range #1 (measured in V)
  - Input voltage range #2 (if necessary; measured in V)
  - Input frequency range (measured in Hz)
  - Part number
  - Serial number
  - Hardware revision for the specified power supply (if one is specified)
  - Range of power supplies, or for all power supplies (if ALL is specified).

- **Access level/Bay level:**
  All

- **Restrictions:**
  None

- **Example:**
  OA-0018FE27577F> show enclosure powersupply 1  
  Power Supply #1 Information:  
  Status: OK  
  AC Input Status: OK
SHOW ENCLOSURE STATUS

- **Command:**
  SHOW ENCLOSURE STATUS

- **Description:**
  Displays the basic health and status of the enclosure subsystem, including the power and cooling subsystems.

  For the cooling subsystem, status of fans is reported as Good/Wanted/Needed, such as 8/8/7.
  
  - **Good** — number of healthy fans detected on the enclosure.
  
  - **Wanted** — number of fans (4, 6, 8, or 10) recommended to ensure adequate cooling on all devices, based on the number of server blades or interconnects configured. A loss of one fan is generally tolerable. When the number of good fans is less than the number of wanted fans but greater than or equal to the number of needed fans, a warning condition exists.
  
  - **Needed** — minimum (tolerable) number of fans required to ensure adequate cooling on all devices. When the number of good fans is less than the number of needed fans, a failure condition exists.

- **Access level/Bay level:**
  All

- **Restrictions:**
  None

- **Example:**
  
  OA-0018FE27577F> SHOW ENCLOSURE STATUS
  Enclosure:
  Status: OK
  Unit Identification LED: Off
  Diagnostic Status:
  Internal Data OK
  Redundancy OK

  Onboard Administrator:
  Status: OK

  Power Subsystem:
  Status: OK
  Power Mode: Redundant
  Redundancy State: Redundant
  Power Capacity: 6750 Watts DC
  Power Available: 4089 Watts DC
  Present Power: 2096 Watts AC

  Cooling Subsystem:
  Status: OK
Fans Good/Wanted/Needed: 6/6/5
Fan 1: 17307 RPM (96%)
Fan 2: 17292 RPM (96%)
Fan 3: Fan Slot Empty
Fan 4: 9446 RPM (52%)
Fan 5: 9437 RPM (52%)
Fan 6: 6902 RPM (38%)
Fan 7: 6903 RPM (38%)
Fan 8: Fan Slot Empty
Fan 9: 8006 RPM (44%)
Fan 10: 8007 RPM (44%)

SHOW ENCLOSURE TEMP

- **Command:**
  SHOW ENCLOSURE TEMP

- **Description:**
  Displays the highest ambient temperature being reported by the installed blade devices. If no blade devices are installed, displays the temperature of the OA module as an approximation of the ambient temperature.

- **Access level/Bay level:**
  All
  Bay specific

- **Restrictions:**
  None

- **Example:**
  OA-0018FE27577F> SHOW ENCLOSURE TEMP

<table>
<thead>
<tr>
<th>Locale</th>
<th>Temp Status</th>
<th>Temp</th>
<th>Caution</th>
<th>Critical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enclosure</td>
<td>N/A</td>
<td>26C/ 78°F</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Onboard Administrator</td>
<td>1 OK</td>
<td>26C/ 78°F</td>
<td>75C</td>
<td>80C</td>
</tr>
<tr>
<td>Blade Bay</td>
<td>7 N/A</td>
<td>20C/ 68°F</td>
<td>38C</td>
<td>43C</td>
</tr>
<tr>
<td>Blade Bay</td>
<td>8 N/A</td>
<td>25C/ 77°F</td>
<td>45C</td>
<td>60C</td>
</tr>
<tr>
<td>Blade Bay</td>
<td>2A N/A</td>
<td>25C/ 77°F</td>
<td>40C</td>
<td>45C</td>
</tr>
<tr>
<td>Blade Bay</td>
<td>2B N/A</td>
<td>27C/ 80°F</td>
<td>40C</td>
<td>45C</td>
</tr>
<tr>
<td>Interconnect Module</td>
<td>1 OK</td>
<td>----</td>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>

SHOW FRU

- **Command:**
  SHOW FRU

- **Description:**
  - The FRU Summary section provides information on all field replaceable units within the enclosure.
  - Information provided in this section can quickly aid the administrator in contacting HP Customer Service for troubleshooting, repair, and ordering replacements.

- **Access level/Bay level:**
All

Bay specific

- **Restrictions:**
  You must have access to the specified bay.

- **Example:**

  OA-0018FE27577F> show fru

Enclosure

  Model: BladeSystem c3000 Enclosure
  Manufacturer: HP
  Serial Number: 0987654321
  Part Number: 437506-B21

Enclosure Midplane

  Manufacturer: HP
  Spare Part Number: 441829-001

Onboard Administrator 1

  Model: BladeSystem c3000 Onboard Administrator
  Manufacturer: HP
  Serial Number: P30590A9VUQ04B
  Part Number: 448589-B21
  Spare Part Number: 441832-001
  Firmware Version: 2.40
  HwVersion: A0

Blade 1

  Model: ProLiant BL480c G1
  Manufacturer: HP
  Serial Number: USM64204B1
  Part Number: 416667-B21
  Spare Part Number: 410293-001

Blade 2

  Model: Integrity BL860c
  Manufacturer: hp
  Serial Number: CSJ0634214
  Part Number: AD323A
  Spare Part Number: AD217-60001

Blade 7

  Model: ProLiant BL460c G1
  Manufacturer: HP
  Serial Number: USM62401EP
  Part Number: 404664-B21
  Spare Part Number: 410299-001

Interconnect 1

  Model: GbE2c Ethernet Blade Switch
  Manufacturer: HP
  Serial Number: MY36290EMT
  Part Number: 410917-B21
  Spare Part Number: 414037-001

Interconnect 2

  Model: HP 1/10Gb VC-Enet Module
Manufacturer: HP
Serial Number: TW2702004K
Part Number: 399593-B22
Spare Part Number: 399725-001

Fan 1
Model: Active Cool 200 Fan
Part Number: 412140-B21
Spare Part Number: 413996-001

Fan 2
Model: Active Cool 200 Fan
Part Number: 412140-B21
Spare Part Number: 413996-001

Fan 3
Model: Active Cool 200 Fan
Part Number: 412140-B21
Spare Part Number: 413996-001

Fan 4
Model: Active Cool 200 Fan
Part Number: 412140-B21
Spare Part Number: 413996-001

Fan 5
Model: Active Cool 200 Fan
Part Number: 412140-B21
Spare Part Number: 413996-001

Fan 6
Model: Active Cool 200 Fan
Part Number: 412140-B21
Spare Part Number: 413996-001

Power Supply 1
Model: 438203-001
Serial Number: 531300ALL00233
Spare Part Number: XXXXXX-001

Power Supply 2
Model: 438203-001
Serial Number: 531300ALL00014
Spare Part Number: XXXXXX-001

Power Supply 3
Model: 438203-001
Serial Number: 531300ALL00399
Spare Part Number: XXXXXX-001

Insight Display
Model: BladeSystem c3000 Insight Display
Manufacturer: HP
Spare Part Number: 441831-001
Firmware Version: 2.2.2
SHOW LANGUAGES

- **Command:**
  SHOW LANGUAGES

- **Description:**
  Displays all language support packs installed. Language support packs enable the Onboard Administrator GUI to display information in languages other than English.

- **Access level/Bay level:**
  OA administrator, OA operator, OA user

- **Restriction:**
  None

- **Example:**
  OA-E4115BECFBAB> show languages

  Found 2 language support pack(s). Language support packs enables OA GUI to display information in languages other than English.

<table>
<thead>
<tr>
<th>Language</th>
<th>Version</th>
<th>Date</th>
<th>Code</th>
<th>File name</th>
</tr>
</thead>
<tbody>
<tr>
<td>English</td>
<td>4.10</td>
<td>Nov 06 2013</td>
<td>en</td>
<td>Embedded</td>
</tr>
<tr>
<td>Chinese</td>
<td>4.10</td>
<td>Sep 30 2013</td>
<td>zh</td>
<td>OA_410_130930_zh.lpk</td>
</tr>
</tbody>
</table>

SHOW OA

- **Command:**
  SHOW OA {CERTIFICATE | INFO | NETWORK | STATUS | UPTIME | USB} [ALL | <bay number> [{, | - } <bay number>] | ACTIVE | STANDBY]

- **Description:**
  - Displays the certificate information, network configuration, status, uptime, or USB mode of the Onboard Administrator.
  - If you do not specify the Onboard Administrator (ALL, <bay number>, ACTIVE, or STANDBY), the command displays information pertaining to the current (local) Onboard Administrator.

- **Access level/Bay level:**
  All

- **Restrictions:**
  None

SHOW OA CERTIFICATE

- **Command:**
  SHOW OA CERTIFICATE [ALL | <bay number> [{, | - } <bay number>] | ACTIVE | STANDBY]
• **Description:**
  o Shows the certificate information for the Onboard Administrator.
  o If you do not specify the Onboard Administrator (ALL, <bay number>, ACTIVE, or STANDBY), the command displays certificate information for the current (local) Onboard Administrator.

• **Access level/Bay level:**
  All

• **Restrictions:**
  None

• **Example:**
  OA-0018FE27577F> SHOW OA CERTIFICATE
  Onboard Administrator #1 Certificate Information:
  - Issued by: OA-0018FE27577F
  - Valid from: 2007-02-01T09:54:30Z
  - Valid until: 2017-01-29T09:54:30Z
  - Serial Number: 1A:TT:66:77:FF:2D
  - Version: 1
  - Subject:
    - Common Name (CN): OA-1234FE27577F
    - Country (C):
    - State or Province (ST):
    - City or Locality (L):
    - Organization Name (O): Hewlett-Packard
    - Organizational Unit: Onboard Administrator

SHOW OA INFO

• **Command:**
  SHOW OA INFO [ALL | <bay number> [{, | - }<bay number>] | ACTIVE | STANDBY]

• **Description:**
  o Displays information about the Onboard Administrator.
  o If you do not specify the Onboard Administrator (ALL, <bay number>, ACTIVE, or STANDBY), the command displays information about the current (local) Onboard Administrator.

• **Access level/Bay level:**
  All

• **Restrictions:**
  None

• **Example:**
  OA-0018FE27577F> SHOW OA INFO
  Onboard Administrator #1 information:
  - Product Name: BladeSystem c3000 Onboard Administrator
  - Part Number: 123456-B21
  - Spare Part No.: 123456-001
  - Serial Number: PLO590A9FDJ8
  - UUID: 123P4R5T6YVUQ04B
  - Manufacturer: HP
SHOW OA NETWORK

• **Command:**
  
  SHOW OA NETWORK [ALL | <bay number> [{, | -} <bay number>] | ACTIVE | STANDBY]

• **Description:**
  
  o Displays the network configuration for the specified Onboard Administrator.
  
  o If you do not specify the Onboard Administrator (ALL, <bay number>, ACTIVE, or STANDBY),
    the command displays information about the current (local) Onboard Administrator.
  
  o If the domain name is set, it is displayed in the output under the "- - - - IPv4 Information
    - - - -" heading.

• **Access level/Bay level:**
  All

• **Restrictions:**
  VLAN ID information appears only when VLAN is enabled.

• **Example:**
  
  OA-E4115BECFBAB> show oa network
  show oa network

  Enclosure Network Settings:

  - - - - IPv6 Information - - - -
  IPv6: Enabled
  DHCPv6: Enabled
  Router Advertisements: Enabled
  Stateless address autoconfiguration (SLAAC): Enabled

  Onboard Administrator #1 Network Information:
  Name: slammer-long-hostname-ie-testing

  - - - - IPv4 Information - - - -
  DHCP: Enabled
  DHCP-Supplied Domain Name: Enabled
  Domain Name: americas.hpqcorp.net
  IPv4 Address: 11.22.333.444
  Netmask: 255.255.252.0
  Gateway Address: 16.84.192.1
  Static IPv4 DNS 1: 11.222.333.52
  Static IPv4 DNS 2: 11.222.333.51

  - - - - IPv6 Information - - - -
  Link-local Address: ff88::e111:5bbb:ffff:ffff/64
SHOW OA STATUS

- **Command:**
  
  SHOW OA STATUS [ALL | <bay number> [{, | - } <bay number>] | ACTIVE | STANDBY]

- **Description:**
  
  o Displays health status for the Onboard Administrator.
  
  o If you do not specify the Onboard Administrator (ALL, <bay number>, ACTIVE, or STANDBY), the command displays health status of the current (local) Onboard Administrator.

- **Access level/Bay level:**
  
  All

- **Restrictions:**
  
  None

- **Example:**
  
  OA-0018FE27577F> SHOW OA STATUS
  
  Onboard Administrator #1 Status:
  
  Name: OA-0018FE27577F
  Role: Active
  UID: Off
  Status: OK
  Diagnostic Status:
  
  Internal Data: OK
  Firmware Mismatch: OK
  OA Battery: OK
SHOW OA UPTIME

- **Command:**
  
  SHOW OA UPTIME [ALL | <bay number> [{, | -} <bay number>] | ACTIVE | STANDBY]

- **Description:**
  - Displays uptime for the Onboard Administrator.
  - If you do not specify the Onboard Administrator (ALL, <bay number>, ACTIVE, or STANDBY), the command displays uptime for the current (local) Onboard Administrator.

- **Access level/Bay level:**
  All

- **Restrictions:**
  None

- **Example:**
  
  OA-0018FE27577F> SHOW OA UPTIME
  
  active all standby
  
  OA-0018FE27577F> SHOW OA UPTIME ACTIVE
  
  Onboard Administrator #1:
  
  Role:     Active
  
  Uptime:   0 days, 0 hours, 43 min
  
  CPU Load: 0.00, 0.02, 0.06

SHOW OA USB

- **Command:**
  
  SHOW OA USB

- **Description:**
  - Displays which USB controller is currently enabled.
  - The **FRONT** controller enables the internal DVD drive and the front USB connector.
  - The **BACK** controller enables the two USB ports on the near KVM Option Module.
  - This command has no effect on HP c3000 Onboard Administrator boards that are hardware revision level C0 and later. Hardware revision is found using the SHOW OA INFO command.

- **Access level/Bay level:**
  All

- **Restrictions:**
  None

- **Example:**
  
  OA-0018FE27577F> SHOW OA USB
  
  Onboard Administrator USB setting = FRONT

SHOW POWER

- **Command:**
  
  SHOW POWER
• **Description:**
  Displays the current power configuration

• **Access level/Bay level:**
  All

• **Restrictions:**
  None

• **Example:**
  OA-0018FE27577F> SHOW POWER
  Power Mode: Not Redundant
  Dynamic Power: Enabled
  Set Power Limit: Not Set
  Power Capacity: 3600 Watts DC
  Power Available: 2685 Watts DC
  Power Allocated: 915 Watts DC
  Present Power: 476 Watts AC
  Power Limit: 4378 Watts AC

**SHOW SYSLOG**

• **Command:**
  SHOW SYSLOG {SERVER <bay number> | ILO <bay number> | ENCLOSURE | OA <bay number> | HISTORY | SETTINGS}

• **Description:**
  Displays the syslog of the enclosure with 22 lines per screen. To quit the command, enter q. Any other key shows the next screen, if there is more information to display.

• **Access level/Bay level:**
  Bay specific
  All

• **Restrictions:**
  You must have access to the specified bay.

• **Example:**
  OA-0016355E560A> SHOW SYSLOG SERVER
  Retrieving Server syslog(s) ...
  Server 1 Syslog:
  <EVENT_LOG DESCRIPTION="Integrated Management Log">
  <EVENT SEVERITY="Informational" CLASS="Maintenance" LAST_UPDATE="02/12/2007 18:01" INITIAL_UPDATE="02/12/2007 18:01" COUNT="1" DESCRIPTION="IML Cleared (iLO user:Administrator)"

  OA-0016355E560A> SHOW SYSLOG ENCLOSURE
  Apr 23 12:25:03  OA: Authentication failure for user larry from 18.84.33.55, requesting authenticate_user
  Apr 23 12:25:13  OA: Authentication failure for user larry from 18.84.33.55, requesting authenticate_user
SHOW SYSLOG OA

- **Command:**
  
  SHOW SYSLOG OA [<bay number>]

- **Description:**
  
  Displays the syslog for the Onboard Administrator. If no bay number is given, then the Active Onboard Administrator syslog appears.

- **Access level/Bay level:**
  
  OA administrator, OA operator, OA user

- **Restrictions:**
  
  None

- **Example:**

  OA-0018FE27577F> SHOW SYSLOG OA

  Apr  2 16:21:22 in.ftpd[25446]: connection from 12.34.567.890
  Apr  2 16:21:24 in.ftpd[25446]: exiting due to EOF from client
  Apr  2 16:21:35 in.ftpd[25451]: connection from 12.34.567.890
  Apr  2 16:21:36 in.ftpd[25451]: exiting due to EOF from client
  Apr  2 16:24:29 in.ftpd[25222]: exiting due to EOF from client
  Apr  2 16:25:01 in.ftpd[25558]: connection from 12.34.567.890
  Apr  2 16:25:02 in.ftpd[25558]: user logged in
  Apr  2 16:25:03 in.ftpd[25559]: connection from 12.34.567.890
  Apr  2 16:25:05 in.ftpd[25559]: userlogged in
  Apr  2 16:25:13 in.ftpd[25559]:
  Apr  2 16:31:44 in.ftpd[25559]:
  Apr  2 16:32:58 OA: Administrator logged into the Onboard Administrator
  Apr  2 16:34:27 in.ftpd[25559]: exiting due to EOF from client
  Apr  2 16:55:02 in.ftpd[25558]: exiting due to timeout (idle time 1800)
  Apr  2 16:59:12 OA: Administrator logged out of the Onboard Administrator
  Apr  2 19:30:05 in.ftpd[31241]: connection from 12.34.567.890
  Apr  2 19:30:07 in.ftpd[31241]: guest logged in
  Apr  2 19:30:12 in.ftpd[31245]: connection from 12.34.567.890
  Apr  2 19:30:13 in.ftpd[31245]: user logged in
  Apr  2 19:30:27 in.ftpd[31245]: Can't change directory to standby.xml: No such file or directory
  Apr  2 19:30:29 in.ftpd[31241]: Can't change directory to standby.xml: No such file or directory
  Apr  2 19:31:09 in.ftpd[31245]:
  Apr  2 19:33:55 in.ftpd[31245]:
SHOW SYSLOG HISTORY

- **Command:**
  
  `SHOW SYSLOG HISTORY <number of entries> [bay number] | ACTIVE | STANDBY`

- **Description:**
  - Displays the extended system log history for the Onboard Administrator. To display all logged entries, use 0.
  - If the Onboard Administrator (`<bay number>`, ACTIVE, or STANDBY) is not specified, the command displays the system log history of the current (local) Onboard Administrator.
  - The Onboard Administrator automatically saves 300 KB of the latest system log history. This extended system log is retained during a reboot, restart, and power off, if those actions are performed gracefully. In optimal circumstances, the Onboard Administrator automatically saves up to 400 KB of the latest system log history. If power to the Onboard Administrator is removed unexpectedly or the Onboard Administrator is removed from the enclosure without a proper shutdown, the latest (unsaved) portions of the extended system log might be lost.
  - You can save the latest system log history by saving the displayed text to a USB drive or other media. Or, use remote system logging; for more information, see "Remote syslog commands (on page 201)."

- **Access level/Bay level:**
  - OA administrator, OA operator, OA user

- **Restrictions:**
  - None

- **Example:**
  
  ```
  OA-0018FE27577F> SHOW SYSLOG HISTORY 20
  Apr 2 16:21:22 in.ftpd[25446]: connection from 12.34.567.890
  Apr 2 16:21:24 in.ftpd[25446]: exiting due to EOF from client
  Apr 2 16:21:35 in.ftpd[25451]: connection from 12.34.567.890
  Apr 2 16:21:36 in.ftpd[25451]: exiting due to EOF from client
  Apr 2 16:24:29 in.ftpd[25222]: exiting due to EOF from client
  Apr 2 16:25:01 in.ftpd[25558]: connection from 12.34.567.890
  Apr 2 16:25:02 in.ftpd[25558]: user logged in
  Apr 2 16:25:03 in.ftpd[25559]: connection from 12.34.567.890
  Apr 2 16:25:05 in.ftpd[25559]: user logged in
  Apr 2 16:25:13 in.ftpd[25559]:
  Apr 2 16:31:44 in.ftpd[25559]:
  Apr 2 16:32:58 OA: Administrator logged into the Onboard Administrator
  Apr 2 16:34:27 in.ftpd[25559]: exiting due to EOF from client
  Apr 2 16:55:02 in.ftpd[25558]: exiting due to timeout (idle time 1800)
  Apr 2 16:59:12 OA: Administrator logged out of the Onboard Administrator
  Apr 2 19:30:05 in.ftpd[31241]: connection from 12.34.567.890
  Apr 2 19:30:07 in.ftpd[31241]: guest logged in
  Apr 2 19:30:12 in.ftpd[31245]: connection from 12.34.567.890
  Apr 2 19:30:13 in.ftpd[31245]: user logged in
  Apr 2 19:30:27 in.ftpd[31245]: Can't change directory to standby.xml: No such file or directory
  ```
**UPDATE**

- **Command:**
  
  UPDATE {IMAGE | ILO | SHOW | DEVICE | FIRMWARE }

- **Description:**
  - The UPDATE SHOW (or SHOW UPDATE) command displays enclosure devices that are available for firmware upgrade.
  - The UPDATE DEVICE command executes the firmware upgrade process on one or more available enclosure devices.
  - The device must be restarted after the firmware update by UPDATE command.
  - The updated firmware version in the NewVersion column is already available in the Onboard Administrator firmware code and does not have to be downloaded from the HP website.

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  - The UPDATE DEVICE FORCE ALL command is not allowed. You can update single devices only by using UPDATE DEVICE FORCE.

  **CAUTION:** When a firmware upgrade is in process, do not disconnect or shut down the Onboard Administrator modules. Doing so could render the Onboard Administrator or server blade unusable.

  **NOTE:** Updating the OA firmware from an OA version earlier than 3.50 to OA version 4.50 or later requires an intermediate update to OA 3.50 first. The intermediate OA 3.50 firmware can be downloaded from the HP Onboard Administrator website (http://h20564.www2.hp.com/hpsc/swd/public/detail?swItemId=MTX_00b278b5e9194e7ab0ab362d55).

- **Notes:**
  - Updating components using this command might interrupt server connectivity.
  - Updating partner blade management firmware requires the corresponding server be powered off first, then the component updated, and then the server can be powered back on.
  - Some components may require power cycling after the firmware update for the new firmware to be activated.
  - The discovery PIC is identified as a BLD string.

- **Example:**
  
  `>update show`

<table>
<thead>
<tr>
<th>Device</th>
<th>Name</th>
<th>Location</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRAY</td>
<td>BladeSystem c7000 Onboard Administrator Tray</td>
<td>-</td>
<td>1.7</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1.7</td>
</tr>
<tr>
<td>ICBAY</td>
<td>HP 1Gb Ethernet Pass-Thru Module for c-Class</td>
<td>1A</td>
<td>2.8.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3.0.3</td>
</tr>
</tbody>
</table>
UPDATE ILO

- **Command:**
  UPDATE ILO {ALL | <bay number> [{, | - } <bay number>]} <url> [TPM_FORCE]

- **Description:**
  - The UPDATE ILO command downloads a new flash image from the network and uses it to update the firmware for iLO.
  - Supported protocols are HTTP, HTTPS, TFTP, and FTP.
  - The URL must be formatted as protocol://host/path/file.
  - If your FTP server does not support anonymous logins, then a user name and password can be specified within the URL formatted as ftp://username/password@host/path/file.
  - If TPM is installed and enabled on the server blade, the UPDATE ILO command must include the TPM_FORCE option after the URL.
  - Upgrading an iLO without performing the proper OS encryption procedure will result in loss of access to your server data if a TPM is enabled. If you do not have your recovery key or have not suspended encryption, do not flash iLO.

- **Access level/Bay level:**
  Administrator
  Blade bay

- **Restrictions:**
  - If maximum users exist in iLO (12), then this command fails. A user account must be available to execute this command.
  - This command is not applicable to HP Integrity server blades.

UPDATE IMAGE FW_ISO

- **Command:**
UPDATE IMAGE ([FORCE] FW_ISO <url> | SYNC)

- **Description:**

  △ **CAUTION:** In FIPS Mode ON/DEBUG, an upgrade to the current version of the Onboard Administrator from a version earlier than 4.35 retains the first 21 local user accounts that were created, including any reserved accounts such as the Administrator or Virtual Connect users. The remainder of the users are deleted.

  - The **IMAGE** command downloads a new flash image from the network and uses it to update the Onboard Administrator firmware. If a redundant Onboard Administrator is present in the system, then this command flashes and validates its firmware before attempting to flash the active Onboard Administrator.

  - Updates the Onboard Administrator firmware using an image on a firmware CD. Enclosure Firmware Management must be configured with a valid ISO URL.

  - Supported protocols are HTTP, FTP, and TFTP.

  - The URL must be formatted as: protocol://host/path/file.

  - The URL syntax for IPv4 addresses is protocol://<ipv4 address>/path/file.

  - The URL syntax for IPv6 addresses is protocol://[<ipv6 address>]/path/file.

  - If your FTP server does not support anonymous connections, you can specify a user name and password in the format ftp://username:password@host/path/file.

  - Use **FORCE** to enable downgrading of firmware even if settings and passwords might be lost.

  - The **UPDATE IMAGE SYNC** command initiates a firmware sync of the Active and Standby Onboard Administrators.

  - For USB protocol, see the **SHOW USBKEY** (on page 204) command.

- **Access level/Bay level:**

  OA administrator, OA operator

- **Restrictions:**

  - You cannot use the **FORCE** option for a downgrade in FIPS Mode ON/DEBUG.

  - The maximum supported file size on USB keys formatted for FAT32 file systems is 4GB. For SPP images greater than 4GB, use an ext2-formatted USB key. For information about formatting a USB key with an ext2 file system, see the **HP BladeSystem Onboard Administrator User Guide**.

  △ **CAUTION:** When a firmware upgrade is in process, do not disconnect or shut down the Onboard Administrator modules. Doing so could render the Onboard Administrator or server blade unusable.

**UPLOAD CONFIG**

- **Command:**

  UPLOAD CONFIG ("<url>" | USB "<filename>")

- **Description:**

  - Uploads to the specified URL a script that duplicates the current runtime configuration.

  - Supported protocols are FTP, TFTP, and USB.

  - Format the URL as follows: protocol://host/path/file.
The URL syntax for IPv4 addresses is protocol://<ipv4 address>/path/file.
The URL syntax for IPv6 addresses is protocol://[<ipv6 address>]/path/file.
If your FTP server does not support anonymous connections, you can specify a user name and
password in the format ftp://username:password@host/path/file.
To save an Onboard Administrator configuration file to a USB key, use the USB keyword and
provide a file name.

- **Access level/Bay level:**
  OA administrator
- **Restriction:**
The user password is not saved or restored by the **UPLOAD** **CONFIG** command.

**UPLOAD SUPPORTDUMP**

- **Command:**
  
  ```plaintext
  UPLOAD SUPPORTDUMP "<url>"
  ```

- **Description:**
  - Uploads supportdump data to the specified URL.
  - Supported protocols are FTP, TFTP, and USB.
  - The URL must be formatted as: protocol://host/path/file.
  - The URL syntax for IPv4 addresses is protocol://<ipv4 address>/path/file.
  - The URL syntax for IPv6 addresses is protocol://[<ipv6 address>]/path/file.
  - If your FTP server does not support anonymous connections, you can specify a user name and
    password in the format ftp://username:password@host/path/file.
  - To upload to the enclosure’s connected USB drive, use the command **UPLOAD SUPPORTDUMP**
    USB://D1/LOG1 (where D is the USB drive letter and 1 is the USB drive number). Up to four USB
    drives are supported, so the number must be between 1 and 4.

- **Access level/Bay level:**
  OA administrator
- **Restriction:**
  You cannot use the **UPLOAD SUPPORTDUMP** command in FIPS Mode ON/DEBUG.

**UPLOAD SYSLOG**

- **Command:**
  
  ```plaintext
  UPLOAD SYSLOG [<URL>]
  ```

- **Description:**
  - Uploads the extended system log history for the current Onboard Administrator.
  - Supported protocols are FTP, TFTP, and USB.
  - The URL must be formatted as: protocol://host/path/file.
  - The URL syntax for IPv4 addresses is protocol://<ipv4 address>/path/file.
  - The URL syntax for IPv6 addresses is protocol://[<ipv6 address>]/path/file.
If your FTP server does not support anonymous connections, you can specify a user name and password in the format ftp://username:password@host/path/file.

- **Access level/Bay level:**
  OA administrator, OA operator, OA user

- **Restrictions:**
  None
Enclosure Firmware Management commands

CLEAR FIRMWARE MANAGEMENT ALL_LOGS

- **Command:**
  CLEAR FIRMWARE MANAGEMENT ALL_LOGS

- **Description:**
  Clears all data from the Enclosure Firmware Management logs, including the Onboard Administrator's Enclosure Firmware Management log, and the server-specific Firmware log and Session log.

  **CAUTION:** Once deleted, this data cannot be restored.

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  None

DISCOVER FIRMWARE SERVER

- **Command:**
  DISCOVER FIRMWARE SERVER {ALL | <bay number> [{- | ,} <bay number>]}]

- **Description:**
  Manual firmware discovery. The blade is reset, which simulates a removal and insertion of the blade.

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  If the server blade in a specified bay is in Secure Boot mode, you cannot perform manual firmware discovery from the Onboard Administrator CLI or GUI. Attempts to use this command result in an error message. The operation can be performed only from the boot device configured in BIOS by the Administrator.

DISABLE FIRMWARE MANAGEMENT

- **Command:**
  DISABLE FIRMWARE MANAGEMENT

- **Description:**
  Disables enclosure firmware management

- **Access level/Bay level:**
  OA administrator
• Restrictions:
  None

ENABLE FIRMWARE MANAGEMENT

• Command:
  ENABLE FIRMWARE MANAGEMENT

• Description:
  Enables enclosure firmware management

• Access level/Bay level:
  OA administrator

• Restrictions:
  None

SET FIRMWARE MANAGEMENT

• Command:
  SET FIRMWARE MANAGEMENT { URL | POLICY | POWER | SCHEDULE | BAYS_TO_INCLUDE | FORCE DOWNGRADE }

• Description:
  Configures various enclosure firmware management settings

• Access level/Bay level:
  OA administrator

• Restrictions:
  None

SET FIRMWARE MANAGEMENT URL

• Command:
  SET FIRMWARE MANAGEMENT URL {DVD | <url> | NONE}

• Description:
  Sets the location on the management network of the HP Firmware ISO image. Supported protocols for
  the URL are HTTP and USB, or the enclosure DVD (specify the DVD keyword). Format the URL as:
  protocol://host/path/file. The URL syntax for IPv6 addresses is protocol://[<ipv6
  address>]/path/file. If Enclosure Firmware Management is disabled, NONE clears the location of
  the HP Firmware ISO image.

• Access level/Bay level:
  OA administrator

• Restrictions:
  o The maximum supported size of the SPP ISO image is 4GB. With SPP ISO images greater than 4GB,
  create a custom ISO image that excludes components unnecessary to the OA EFM blade firmware
  update process. At minimum, the custom ISO must contain only the firmware components for HP
ProLiant BL Series server blades. For information about creating a custom ISO image, see the HP BladeSystem Onboard Administrator User Guide.

To use the complete ISO image with a file size greater than 4GB, you must use an ext2-formatted USB key. For information about formatting a USB key with an ext2 file system, see the HP BladeSystem Onboard Administrator User Guide.

⚠️ **CAUTION:** Enclosure Firmware Management updates using an SPP image greater than 4GB and hosted from a web server might not work reliably.

- The maximum length of the URL is 511 characters.
- If the image is being used, the URL cannot be changed.

### SET FIRMWARE MANAGEMENT POLICY

- **Command:**
  ```
  SET FIRMWARE MANAGEMENT POLICY { MANUAL | AUTO DISCOVER | AUTO UPDATE }
  ```

- **Description:**
  Sets the Enclosure Firmware Management policy for the enclosure. To update and discover manually, use the `MANUAL` option. To automatically discover server firmware on insertion, use the `AUTO DISCOVER` option. To automatically update server firmware on insertion, use the `AUTO UPDATE` option.

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  None

### SET FIRMWARE MANAGEMENT POWER

- **Command:**
  ```
  SET FIRMWARE MANAGEMENT POWER { OFF | POWEROFF | FORCE }
  ```

- **Description:**
  Sets the Enclosure Firmware Management power control policy for the enclosure.

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  - **OFF**—The server must be powered off or the Onboard Administrator cancels the operation. This setting is the default.
  - **POWEROFF**—The Onboard Administrator attempts to softly shut down the server. This is equivalent to pressing the Momentary Press virtual button for the server. If server power remains on for more than five minutes, the Onboard Administrator cancels the operation.
  - **FORCE**—The Onboard Administrator forces an immediate hard shutdown of the server. This is equivalent to pressing the Press and Hold virtual button for the server.
SET FIRMWARE MANAGEMENT SCHEDULE

- **Command:**
  
  ```
  SET FIRMWARE MANAGEMENT SCHEDULE { <YYYY-MM-DD> <HH:MM> | NONE }
  ```

- **Description:**
  Sets the date and time to run a scheduled update. Enclosure Firmware Management must be enabled and a firmware management URL must be specified. Use `NONE` to disable scheduled firmware updates.

- **Access level/Bay level:**
  
  OA administrator

- **Restrictions:**
  
  None

SET FIRMWARE MANAGEMENT BAYS_TO_INCLUDE SERVER

- **Command:**

  ```
  SET FIRMWARE MANAGEMENT BAYS_TO_INCLUDE SERVER { ALL | <bay number> [{, | - } <bay number>] | NONE }
  ```

- **Description:**
  Configures which server bays are included in the Enclosure Firmware Management policy. If bays were included in a previous operation, then you must reselect the bays.

- **Access level/Bay level:**
  
  OA administrator

- **Restrictions:**

  - Bay ranges must be completely specified. Base bays, side a bays, and side b bays cannot be mixed in a single range. Ranges such as 1a-4b or 5-7a are not valid. For example, the following command designates base bays 1 through 5 only. Side a or side b bays are not included:
    ```
    set firmware management bays_to_include server 1-5
    ```
  
  - Multiple ranges must be specified in the same statement, for example:
    ```
    set firmware management bays_to_include server 1-4, 1a-3a, 1b-2b
    ```
  
  - The `bays_to_include` feature only applies to ProLiant server blades. Integrity server blades do not support this feature. Partner blade support is provided through the associated server blade based on whether the firmware ISO supports the PCIe adapter card in the partner blade.

SET FIRMWARE MANAGEMENT FORCE DOWNGRADE

- **Command:**

  ```
  SET FIRMWARE MANAGEMENT FORCE DOWNGRADE { ENABLE| DISABLE }
  ```

- **Description:**
Sets the firmware update force downgrade policy. Enable this option to force all devices to have firmware updated to the version supplied by the ISO, even if a newer version is currently installed on the device. This option is disabled by default.

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  - When forcing a downgrade of the Onboard Administrator to an earlier version of the firmware, current settings that are inapplicable to the earlier version may be lost.
  - When the Onboard Administrator is in VC mode and IPv6 is enabled, the Virtual Connect Manager may specify a minimum expected firmware version for the Onboard Administrator. When this situation occurs, disabling Onboard Administrator IPv6 communication prior to the downgrade attempt makes it possible for VC to interoperate with older Onboard Administrator versions.

### SHOW FIRMWARE

- **Command:**
  SHOW FIRMWARE { MANAGEMENT | SUMMARY | LOG }  
  
- **Description:**
  Displays all the firmware management settings followed by a list of all firmware in the enclosure. It includes a list of the extended server firmware information on all servers that have completed discovery or update.

### SHOW FIRMWARE MANAGEMENT

- **Command:**
  SHOW FIRMWARE MANAGEMENT  
  
- **Description:**
  Displays enclosure firmware management configuration settings

- **Access level/Bay level:**
  All

- **Restrictions:**
  The Firmware ISO Information section is viewable by OA administrator or Administrator only.

- **Example:**
  OA-00215AB0EA21> show firmware management

  Enclosure Firmware Settings

  Enclosure: OA-984BE1601C55
  Firmware Management: Enabled
  - Force Downgrade: Enabled
  - Firmware ISO URL: http://16.84.188.24/mycompany.com/FW.iso
  - Firmware Power Policy: FORCE
  - Firmware Policy: Automatic Update
  - Firmware Date: Not Set
  - Bays to Include
SHOW FIRMWARE MANAGEMENT LOG

- **Command:**
  SHOW FIRMWARE MANAGEMENT LOG

- **Description:**
  Displays the enclosure firmware management log

- **Access level/Bay level:**
  - OA Administrator

- **Restrictions:**
  - None

SHOW FIRMWARE SUMMARY

- **Command:**
  SHOW FIRMWARE SUMMARY

- **Description:**
  Displays a summary of enclosure firmware components. An exclamation mark (!) indicates firmware mismatch or missing firmware information.

- **Access level/Bay level:**
  - All
  - Bay specific

- **Restrictions:**
  - You must have access to the specified bay number.
  - The Enclosure Component Firmware Information section is viewable by OA administrator or Administrator only.

- **Example:**

  Onboard Administrator Firmware Information

<table>
<thead>
<tr>
<th>Bay Model</th>
<th>Firmware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>BladeSystem c3000 Onboard Administrator</td>
<td>4.40</td>
</tr>
</tbody>
</table>

  Enclosure Component Firmware Information

<table>
<thead>
<tr>
<th>Device Name</th>
<th>Location Version</th>
<th>NewVersion</th>
</tr>
</thead>
</table>

Firmware ISO Information:
- ISO URL Status: Valid URL
  - Version: 2012.02.0
  - Name: HP Smart Update Firmware DVD
- ISO OA Version: 3.60
<table>
<thead>
<tr>
<th>TRAY</th>
<th>BladeSystem c3000 Onboard Administrator</th>
<th>-</th>
<th>2.10</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAN</td>
<td>Active Cool 200 Fan</td>
<td>1</td>
<td>2.7.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.7.4</td>
<td></td>
</tr>
<tr>
<td>FAN</td>
<td>Active Cool 200 Fan</td>
<td>2</td>
<td>2.9.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.9.4</td>
<td></td>
</tr>
<tr>
<td>FAN</td>
<td>Active Cool 200 Fan</td>
<td>3</td>
<td>2.7.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.7.4</td>
<td></td>
</tr>
<tr>
<td>FAN</td>
<td>Active Cool 200 Fan</td>
<td>4</td>
<td>2.7.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.7.4</td>
<td></td>
</tr>
<tr>
<td>FAN</td>
<td>Active Cool 200 Fan</td>
<td>5</td>
<td>2.7.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.7.4</td>
<td></td>
</tr>
<tr>
<td>FAN</td>
<td>Active Cool 200 Fan</td>
<td>6</td>
<td>2.7.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.7.4</td>
<td></td>
</tr>
</tbody>
</table>

### Device Firmware Information

**Device Bay:** 1  
**Discovered:** No

<table>
<thead>
<tr>
<th>Firmware Component</th>
<th>Current Version</th>
<th>Firmware ISO</th>
</tr>
</thead>
<tbody>
<tr>
<td>System ROM</td>
<td>[Unknown]</td>
<td>2.23</td>
</tr>
<tr>
<td>Power Management Controller</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Device Bay:** 2  
**Discovered:** No

<table>
<thead>
<tr>
<th>Firmware Component</th>
<th>Current Version</th>
<th>Firmware ISO</th>
</tr>
</thead>
<tbody>
<tr>
<td>System ROM</td>
<td>[Unknown]</td>
<td>2.23</td>
</tr>
<tr>
<td>Power Management Controller</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Device Bay:** 3A  
**Discovered:** No

<table>
<thead>
<tr>
<th>Firmware Component</th>
<th>Current Version</th>
<th>Firmware ISO</th>
</tr>
</thead>
<tbody>
<tr>
<td>System ROM</td>
<td>I29 07/02/2013</td>
<td></td>
</tr>
<tr>
<td>iLO3</td>
<td>1.80 Jul 01 2014</td>
<td></td>
</tr>
<tr>
<td>Power Management Controller</td>
<td>1.6</td>
<td></td>
</tr>
</tbody>
</table>

**Device Bay:** 3B  
**Discovered:** No
SHOW FIRMWARE SUMMARY CSV

• **Command:**
  SHOW FIRMWARE SUMMARY CSV

• **Description:**
  Displays a summary of enclosure firmware components in comma separated value format. An exclamation mark (!) indicates firmware mismatch or missing firmware information. If the CSV keyword is used, the summary will be output in CSV format.

• **Access level/Bay level:**
  o All
  o Bay specific

• **Restrictions:**
  You must have access to the specified bay number.

• **Example:**
  OA-00215AB0EA21> show firmware summary csv
  Bay Number, Device Name, Discovered, Firmware Component, Current Version, Firmware ISO Version
  1, ProLiant BL495c G5, No, System ROM, A14 12/09/2009, , iLO2, 1.82 Mar 31 2010, , Power Management Controller, ,
  2, ProLiant BL460c G6, Tue 2010-09-14 09:33:55, System ROM, I24 2010.03.30, I24 2010.03.30, ILO2, 2.01, 1.82, Power, 3.4, 3.4, HP NC532i Dual Port 10GbE Multifunction BL-c Adapter, Boot code: 5.2.7, Boot code: 5.2.7, HP NC532i Dual Port 10GbE Multifunction BL-c Adapter, iSCSI: 3.1.5, iSCSI: 3.1.5, Smart Array P410i, 3.00, 3.00, , DG072BB975 (Bay 0), HPDD, ,
  3, ProLiant BL495c G5, Mon 2010-09-13 17:19:34, System ROM, A14 2009.12.09, A14 2009.12.09, ILO2, 1.81, 1.82, Power Management Controller, ERROR, ,
  4, ProLiant BL465c G1, Mon 2010-09-13 17:21:30, System ROM, A13 2009.12.08, A13 2009.12.08, ILO2, 1.82, 1.82, Power Management Controller, 0.5, , HP NC370i Multifunction Gigabit Server Adapter, Boot code: 1.9.6, Boot code: 1.9.6, Smart Array E200i, 1.86, 1.86,
  5, ProLiant BL460c G1, Mon 2010-09-13 17:19:48, System ROM, I15 2009.07.10, I15 2009.07.10, ILO2, 1.70, 1.82, Power Management Controller, , HP NC373i Multifunction Gigabit Server Adapter, Boot code: 4.4.1, Boot code: 4.4.1, HP NC373i Multifunction Gigabit Server Adapter, CLP: 1.3.6, CLP: 1.3.6, HP NC373i Multifunction Gigabit Server Adapter, Boot code: 4.4.1, Boot code: 4.4.1, HP NC373i Multifunction Gigabit Server Adapter, CLP: 1.3.6, CLP: 1.3.6, Smart Array E200i, 1.86, 1.86, , DG036A9BB6 (Bay 0), HPDD, ,
  6A, ProLiant BL2x220c G5, Mon 2010-09-13 17:20:10, System ROM, I19 2009.07.10, I19 2009.07.10, ILO2, 1.79, 1.82, Power Management Controller, 0.5, ,
  6B, ProLiant BL2x220c G5, Mon 2010-09-13 17:24:17, System ROM, I19 2009.07.10, I19 2009.07.10, ILO2, 1.79, 1.82, Power Management Controller, 0.5, ,
  9, ProLiant BL460c G1, No, System ROM, I15 11/13/2007, , ILO2, 1.79 Aug 28 2009, , Power Management Controller, ,
  11, ProLiant BL460c G1, No, System ROM, I15 07/10/2009, , ILO2, 1.81 Jan 15 2010, , Power Management Controller, ,
  12, ProLiant BL495c G6, Mon 2010-09-13 17:18:28, System ROM, A14 2009.12.09, A14 2009.12.09, ILO2, 1.81, 1.82, Power Management Controller, ERROR, , HP NC532i Dual Port 10GbE Multifunction BL-c Adapter, Boot code: 5.2.7, Boot code: 5.2.7, HP NC532i Dual Port 10GbE Multifunction BL-c Adapter, iSCSI: 3.1.5, iSCSI: 3.1.5,
SHOW FIRMWARE LOG SERVER

- **Command:**
  SHOW FIRMWARE LOG SERVER { ALL | <bay number> [{ , | - } <bay number>] }

- **Description:**
  Displays the firmware log for the selected server or range of servers.

- **Access level/Bay level:**
  - All
  - Bay specific

- **Restrictions:**
  You must have access to the specified bay number.

- **Example:**
  OA-00215AB0EA21> show firmware log server 5

Bay 5 firmware log
Sep 13 17:09:01 Started session with iLO2.
Sep 13 17:09:01 Powering off blade with button press.
Sep 13 17:09:11 Blade successfully powered off.
Sep 13 17:09:11 Powering on blade with button press.
Sep 13 17:09:21 Blade has powered on.
Sep 13 17:09:24 Connected to Virtual Serial Port.
Sep 13 17:09:26 Inserted http://mycompany.com/DVD.iso into virtual CD-ROM.
Sep 13 17:09:26 Booting virtual CD-ROM.
Sep 13 17:10:03 Loading firmware image.
Sep 13 17:19:43 Update blade firmware successfully completed.
Sep 13 17:19:43 Blade has been rebooted.
Sep 13 17:19:45 Disconnect from Virtual Serial Port.
Sep 13 17:19:46 Terminated iLO2 session.
Sep 13 17:19:48 Firmware Management successfully completed.

SHOW FIRMWARE LOG SESSION

- **Command:**
  SHOW FIRMWARE LOG SESSION { ALL | <bay number> [{ , | - } <bay number>] }

Enclosure Firmware Management commands 165
• **Description:**
  Displays the firmware log session for the selected server or range of servers

• **Access level/Bay level:**
  - All
  - Bay specific

• **Restrictions:**
  You must have access to the specified bay number.

### SHOW SERVER FIRMWARE

• **Command:**
  `SHOW SERVER FIRMWARE { ALL | <bay number> [( , | - ) <bay number>]]`

• **Description:**
  Displays a summary of firmware components in the specified server or range of servers. An exclamation mark (!) indicates firmware mismatch or missing firmware information.

• **Access level/Bay level:**
  - All
  - Bay specific

• **Restrictions:**
  - You must have access to the specified bay number.
  - Different sides of the server bay cannot be designated within the same range.

• **Example:**
  OA-00215AB0EA21> show server firmware 5

  Device Firmware Information

  Device Bay: 5
  Discovered: Mon 2010-09-13 17:19:48

<table>
<thead>
<tr>
<th>Firmware Component</th>
<th>Current Version</th>
<th>Firmware ISO Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>System ROM</td>
<td>I15 2009.07.10</td>
<td>I15 2009.07.10</td>
</tr>
<tr>
<td>ILO2</td>
<td>1.70</td>
<td>1.82</td>
</tr>
<tr>
<td>Power Management Controller</td>
<td>3.4</td>
<td>3.4</td>
</tr>
<tr>
<td>HP NC373i Multifunction Gigabit Server</td>
<td>Boot code: 4.4.1</td>
<td>Boot code: 4.4.1</td>
</tr>
<tr>
<td></td>
<td>CLP: 1.3.6</td>
<td>CLP: 1.3.6</td>
</tr>
<tr>
<td>HP NC373i Multifunction Gigabit Server</td>
<td>Boot code: 4.4.1</td>
<td>Boot code: 4.4.1</td>
</tr>
<tr>
<td></td>
<td>CLP: 1.3.6</td>
<td>CLP: 1.3.6</td>
</tr>
<tr>
<td>Smart Array E200i</td>
<td>1.86</td>
<td>1.86</td>
</tr>
<tr>
<td>- DG036A9BB6 (Bay 0)</td>
<td>HPD0</td>
<td></td>
</tr>
</tbody>
</table>

### UPDATE FIRMWARE SERVER

• **Command:**
  `UPDATE FIRMWARE SERVER {ALL | <bay number> [( , | - ) <bay number>]]`
• **Description:**
  Initiates manual update of the selected servers, using the configured HP firmware ISO image URL.

  **IMPORTANT:** While any Enclosure Firmware Management task is in progress, do not reboot the Onboard Administrator. Avoid shutting down or pulling out the blade from the enclosure.

• **Access level/Bay level:**
  OA administrator

• **Restrictions:**
  o You must have access to the specified bay number.
  o If the server blade in a specified bay is in Secure Boot mode, you cannot perform this operation from the Onboard Administrator CLI or GUI. Attempts to use this command result in an error message. The operation can be performed only from the boot device configured in BIOS by the Administrator.
ASSIGN SERVER

- **Command:**
  ASSIGN SERVER {ALL | <bay number> [ { , | - } <bay number> | LDAP GROUP "<LDAP group name>" ]}

- **Description:**
  Assigns control of the specified servers to the user or LDAP group.

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  None

CONNECT SERVER

- **Command:**
  CONNECT SERVER [SERIAL] <bay number>

- **Description:**
  Opens a Text Console session to the iLO specified. If the optional argument SERIAL is specified, a Virtual Serial Port session is started.

- **Access level/Bay level:**
  All
  Bay specific

- **Restrictions:**
  The User privilege level cannot use the CONNECT SERVER SERIAL command. User accounts don't have console privileges.

HPONCFG

- **Command:**
  HPONCFG [NOAUTOLOGIN] [SUBSTITUTE [TEST] {“variable”=”value” [,”variable”=”value”[,...]]} {ALL | <bay number> [ { , | - } <bay number> ]} {<< <end marker> \n | <from_url> [<to_url>]\n <end marker>}

- **Description:**
  Sends a RIBCL iLO configuration script to the specified HP ProLiant server blades with the access level and privilege of the current user. The script is an XML file. To use the login credentials in the script as is, specify NOAUTOLOGIN.
To use variable substitution, specify the `SUBSTITUTE` keyword followed by a list of variable assignments. The list of variable assignments must be a string that contains each variable name and its corresponding value. Each variable assignment (the variable name and assigned value) must be separated by an equal sign (=), and the name and the value should each be enclosed by double quotes. Separate multiple key value pairs with a `,` (comma) delimiter.

You can download the script from a FTP, TFTP, HTTP, or HTTPS URL (`<from_URL>`). You can upload the results to a TFTP or FTP location (`<to_URL>`).

To manually enter a RIBCL:

1. Type "<<" followed by a space.
2. Enter a string that does not appear within the RIBCL script (the end marker).
3. Enter a newline character by pressing `ENTER`.
4. Paste the RIBCL script.
5. Enter a newline character by pressing `ENTER`.
6. Finish the command with the end marker.

To view the RIBCL script that will be sent to the iLO, specify `TEST`.

- **Access level/Bay level:**
  - All
  - Bay specific

- **Restrictions:**
  - You must have access to the specified bays.
  - For the iLO Update_Firmware script, the Onboard Administrator must be able to download the iLO firmware file referenced in the script within 2 minutes.
  - This command is not applicable to HP Integrity server blades.
  - To use variable substitution, HPONCFG 1.2 or greater is required. Variables must be specified in the XML RIBCL script before executing the HPONCFG command. Anything enclosed by two `%` characters in the XML file is considered a variable.
  - Quotes are required for strings containing spaces.
  - Variable assignments:
    - Variable name and the value can include spaces, numbers, or any printable characters.
    - Up to 25 variables are supported.
    - The maximum length of a variable name is 48 characters.
    - The maximum length of a variable value is 256 characters.

- **Example:**

  The following command specifies an iLO configuration script for bay 1, using variable substitution. The end marker is "EOF". The `TEST` command displays the RIBCL script, and so the script is not executed.

  ```
  OA-9C8E99224631 [SCRIPT MODE]> HPONCFG SUBSTITUTE TEST
  "username"="riosa","user"="riosa","password"="password" 1 << EOF
  <RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="%s" PASSWORD="%s">
  <USER_INFO MODE="write">
  <ADD_USER USER_NAME="%username%" USER_LOGIN="%user%" PASSWORD="%password%">
  </ADD_USER>
  </USER_INFO>
  </LOGIN>
  </RIBCL>
  ```

---

To view the RIBCL script that will be sent to the iLO, specify `TEST`.
Bay 1: Resulting RIBCL script.
<RIBCL VERSION="2.0">
.LOGIN USER_LOGIN="hiddenValue" PASSWORD="hiddenValue">
,<USER_INFO MODE="write">
<ADD_USER USER_NAME="riosa" USER_LOGIN="riosa" PASSWORD="password">
</ADD_USER>
</USER_INFO>
</LOGIN>
</RIBCL>

POWEROFF SERVER

⚠️ **CAUTION:** This command can cause a server blade to lose data or become unstable.

- **Command:**
  
  POWEROFF SERVER {ALL | <bay number> {{ - | , } <bay number>}} [FORCE]

- **Description:**
  - Performs a graceful shutdown of the server in the specified bay.
  - This command returns the user to the CLI immediately but the shutdown actions can take up to 5 minutes to complete.
  - If the **FORCE** argument is given, the server blade is immediately shut down and might lose data or become unstable.
  - If no blade is in the specified bay, you are notified that the bay is empty.

- **Access level/Bay level:**
  - Administrator, operator
  - Bay specific

- **Restrictions:**
  - You must have access to the specified bay number.
  - This command is not applicable to storage blades. The **FORCE** argument is only valid for server bays.

POWERON SERVER

- **Command:**
  
  POWERON SERVER {ALL | <bay number> {{ - | , } <bay number>}} {{NORMAL | PXE | HDD | RBSU | CD | FLOPPY | USB}}

- **Description:**
  - Powers on the specified server blade or all server blades.
• Adding an optional boot argument forces the server blade to abandon the regular boot order and boot using the specified method.
• If no blade is in the specified bay, you are notified that the bay is empty.

**Access level/Bay level:**
Administrator, operator
Bay specific

**Restrictions:**
• You must have access to the specified bay number.
• This command is not applicable to storage blades.

---

**REBOOT SERVER**

**Command:**
REBOOT SERVER { ALL | <bay number> [{ , | - } <bay number>] } [FORCE] [{ NORMAL | PXE | HDD | RBSU | CD | Floppy | USB }]

**Description:**
• Sends a request to the server to perform a system reset.
• If the **FORCE** option is specified, a request is sent to the server to perform a cold boot resulting in the server being power cycled.
• When a one-time boot device is specified, the server boots to the target device on the resulting server reboot.

⚠️ **WARNING:** Executing this command does not provide the server OS the opportunity to perform a graceful shutdown.

**Access level/Bay level:**
Administrator, operator
Bay specific

**Restrictions:**
• You must have access to the specified bay number.
• This command is not applicable to storage blades.

---

**SET NIC**

**Command:**
SET NIC {AUTO | FORCED}

**Description:**
Configures the external NIC for Auto-negotiation or forced link settings.

**Access level/Bay level:**
OA administrator, OA operator

**Restrictions:**
None
SET SERVER BOOT

- **Command:**
  
  SET SERVER BOOT {FIRST | ONCE} {({NORMAL | CD | HDD | PXE | RBSU | FLOPPY | USB | UEFI_SHELL}) {ALL | <bay number> [{, | - } <bay number>]}} | {UEFI_TARGET <device id> <bay number>}}

- **Description:**
  
  - Stores a setting for the IPL to be passed to the specified servers at the next reboot.
  - SET SERVER BOOT FIRST (on page 172) sets the boot order of the blade.
  - SET SERVER BOOT ONCE (on page 173) sets the boot device to be used on the next boot of the bays specified.

- **Access level/Bay level:**
  
  OA administrator, OA operator
  
  Bay specific

- **Restrictions:**
  
  - You must have access to the specified bay number.
  - This command is not applicable to storage blades.
  - This command is not applicable to HP Integrity server blades.
  - If the server blade in a specified bay is in Secure Boot mode, you cannot perform this operation from the Onboard Administrator CLI or GUI. Attempts to use this command results in an error message. The operation can be performed only from the boot device configured in BIOS by the Administrator.
  - The RBSU, NORMAL, and UEFI_SHELL options are only available for SET SERVER BOOT ONCE.
  - This setting is only valid on present blades and cleared if the blade is removed.
  - UEFI_SHELL and UEFI_TARGET options are available only for UEFI-capable blades.
  - UEFI_TARGET is applicable only for UEFI-capable blades in UEFI boot mode and can be applied to only one blade at a time.
  - The <device id> is valid only for UEFI_TARGET option and can be obtained from the output of the SHOW SERVER BOOT command.

SET SERVER BOOT FIRST

- **Command:**
  
  SET SERVER BOOT FIRST {{HDD | PXE | CD | FLOPPY | USB} {ALL | <bay number> [{, | - } <bay number>]}} | {UEFI_TARGET <device id> <bay number>}}

- **Description:**
  
  - Sets the boot device to be used on the next boot of the bays specified.
  - Stores a setting for the IPL to be passed to the specified servers at the next reboot.
  - HDD sets the boot order of the blade to Hard Disk Drive.
  - PXE sets the boot order of the blade to Preboot Execution Environment.
  - UEFI_TARGET sets the target UEFI device with <device id> as the boot device to be used on the next boot.
• **Access level/Bay level:**
  OA administrator, OA operator
  Bay specific

• **Restrictions:**
  o You must have access to the specified bay number.
  o This command is not applicable to storage blades.
  o This command is not applicable to HP Integrity server blades.
  o This setting is valid only on present blades and is cleared if the blade is removed.
  o If the server blade in a specified bay is in Secure Boot mode, you cannot perform this operation from the Onboard Administrator CLI or GUI. Attempts to use this command result in an error message. The operation can be performed only from the boot device configured in BIOS by the Administrator.
  o **UEFI_TARGET** is applicable only for UEFI-capable blades in UEFI boot mode and can be applied to only one blade at a time.
  o The `<device id>` is valid only for UEFI_TARGET option and can be obtained from the output of the **SHOW SERVER BOOT** command.

### SET SERVER BOOT ONCE

• **Command:**
  ```
  SET SERVER BOOT ONCE {{ NORMAL | HDD | FLOPPY | PXE | RBSU | CD | USB | UEFI_SHELL} {ALL | <bay number> [{ , | - } <bay number>] | { UEFI_TARGET <devIce id> <bay number> ]}
  ```

• **Description:**
  o Sets the boot device to be used on the next boot of the bays specified.
  o Stores a setting for the IPL to be passed to the specified servers at the next reboot.
  o **HDD** sets Hard Disk Drive as the boot device to be used on the next boot.
  o **PXE** sets the PXE Server as the boot device to be used on the next boot.
  o **RBSU** sets the ROM Based Setup Utility as the boot device to be used on the next boot.
  o **UEFI_SHELL** sets the ROM Based Setup Utility as the boot device to be used on the next boot.
  o **UEFI_TARGET** sets the blade server to boot to Embedded UEFI Shell on the next boot.
  o **UEFI_TARGET** sets the target UEFI device with `<device id>` as the boot device to be used on the next boot.

• **Access level/Bay level:**
  OA administrator, OA operator
  Bay specific

• **Restrictions:**
  o You must have access to the specified bay number.
  o This command is not applicable to storage blades.
  o This command is not applicable to HP Integrity server blades.
  o This setting is valid only on present blades and is cleared if the blade is removed.
If the server blade in a specified bay is in Secure Boot mode, you cannot perform this operation from the Onboard Administrator CLI or GUI. Attempts to use this command result in an error message. The operation can be performed only from the boot device configured in BIOS by the Administrator.

- **UEFI_SHELL** and **UEFI_TARGET** options are available only for UEFI-capable blades.
- **UEFI_TARGET** option is available only in UEFI boot mode and can be applied to only one blade at a time.
- The `<device id>` is valid only for **UEFI_TARGET** option and can be obtained from the output of the **SHOW SERVER BOOT** command.

### SET SERVER POWERDELAY

- **Command:**
  
  ```
  SET SERVER POWERDELAY {ALL | <bay number> [{- | , } <bay number>] } {number of seconds to delay power | NOPOWERON}
  ```

- **Description:**
  
  Set the PowerDelay status for the specified server or range of servers. If the delay is zero, the delay has no effect on the device. If the delay is **NOPOWERON**, the device cannot poweron until all devices have completed their delays.

- **Access level/Bay level:**
  
  Administrator
  
  Bay specific

- **Restrictions:**
  
  You must have access to the specified bay number.

### SET SERVER UID

- **Command:**
  
  ```
  SET SERVER UID {ALL | <bay number> [{- | , } <bay number>] } {ON | OFF}
  ```

- **Description:**
  
  Turns a server blade UID LED on or off

- **Access level/Bay level:**
  
  All
  
  Bay specific

- **Restrictions:**
  
  You must have access to the specified bay number.

### SHOW SERVER BOOT

- **Command:**
  
  ```
  SHOW SERVER BOOT {ALL | <bay number> [{- | , } <bay number>] }
  ```

- **Description:**
  
  Displays the boot settings for the specified servers.
• **Access level/Bay level:**
  
  All
  Bay specific

• **Restrictions:**
  o You must have access to the specified bay.
  o This command is not applicable to HP Integrity server blades.
  o Different sides of the server bay cannot be designated within the same range.

• **Example:**

  Command output for a UEFI-capable server blade in UEFI boot mode:
  
  OA-FC15B41A561B> show server boot 1

  Server Blade #1 Boot Information:
  
  One time boot from: Not Set
  IPL Devices (Boot Order):
  
  Device ID.Device Description
  10. Embedded FlexibleLOM 1 Port 1 : HP FlexFabric 10Gb 2-port 536FLB Adapter - CNA (IPv4)
  9. Embedded FlexibleLOM 1 Port 1 : HP FlexFabric 10Gb 2-port 536FLB Adapter - CNA (IPv6)
  8. iLO Virtual USB 2 : HP iLO Virtual USB CD/DVD ROM

  Command output for a server that is not UEFI-capable or that is UEFI-capable in Legacy boot mode:
  
  OA-FC15B41A561B> show server boot 10

  Server Blade #10 Boot Information:
  
  One time boot from: Not Set
  IPL Devices (Boot Order):
  
  PXE NIC 1
  Hard Drive (C:)
  Diskette Drive (A:)
  CD-ROM
  USB
  PXE NIC 2

**SHOW SERVER INFO**

• **Command:**

  SHOW SERVER INFO {ALL | <bay number> [{, | -} <bay number>]}  

• **Description:**

  Displays the following fields:
  o Type
  o Name
  o Part number
  o Serial number
  o Server name
  o Asset tag
  o ROM BIOS version
  o Boot mode (reported only for UEFI-capable server blades)
- Secure Boot status (not reported for UEFI-capable blades running in Legacy boot mode or for Gen8 blades and earlier generations); for more information about Secure Boot, see the *HP UEFI System Utilities User Guide* on the HP website (http://www.hp.com/go/ProLiantUEFI/docs)
- All CPU types and associated maximum speeds
- Memory
- NICs name and slot number
- iLO name, IP address, firmware version
- Power Management Controller version
- iLO Federation capability
- VLAN ID
- IPv6 information
- **Access level/Bay level:**
  - All
  - Bay specific
- **Restrictions:**
  - You must have access to the specified bay number.
  - MAC and WWN information is no longer included in the output for this command with Onboard Administrator firmware version 3.60.
  - Different sides of the server bay cannot be designated within the same range.
- **Example:**
  ```
  OA-984BE179846D> show server info 11
  ```
  **Server Blade #11 Information:**
  - Type: Server Blade
  - Manufacturer: HP
  - Product Name: ProLiant BL460c G7
  - Part Number: 603591-B21
  - System Board Spare Part Number: 605659-001
  - Serial Number: MXQ1281CFX
  - UUID: 33333333-4444-584D-5131-323831434658
  - Server Name: host is unnamed
  - Asset Tag: [Unknown]
  - ROM Version: I27 05/05/2011
  - CPU 1: Intel(R) Xeon(R) CPU E5506 @ 2.13GHz (4 cores)
  - CPU 2: Not present
  - Memory: 6144 MB

  **FlexFabric Embedded Ethernet**
  - Ethernet LOM:2-a 9A:8B:99:1F:CA:34
  - FCoE HBA LOM:2-b 11:22:9C:8E:99:1F:CA:

  This server does not contain any mezzanine cards

  **Management Processor Information:**
SHOW SERVER LIST

- **Command:**
  SHOW SERVER LIST [IPV6]

- **Description:**
  - Displays a brief description of all server blades to which the current user has access
  - Displays by default IPv4 information; to display IPv6 information, enter the **IPV6** keyword

- **Access level/Bay level:**
  - All
  - Bay specific

- **Restrictions:**
  - You must have access to the specified bay number.
  - Use the **IPV6** keyword to display IPv6 address and address type only.

- **Example:**
  OA-0018FE27577F> SHOW SERVER LIST

<table>
<thead>
<tr>
<th>Bay</th>
<th>iLO Name</th>
<th>iLO IP Address</th>
<th>Status</th>
<th>Power</th>
<th>UID</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>[Absent]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>ILOMXQ1281CDZ</td>
<td>111.222.33.444</td>
<td>OK</td>
<td>On</td>
<td>Off</td>
</tr>
</tbody>
</table>

Totals: 1 server blades installed, 0 powered on.

OA-0018FE27577F> SHOW SERVER LIST IPV6

<table>
<thead>
<tr>
<th>Bay</th>
<th>iLO Name</th>
<th>iLO IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Blade management commands 177
SHOW SERVER NAMES

• Command:
  SHOW SERVER NAMES

• Description:
  Displays a brief description of all server blades to which the current user has access

• Access level/Bay level:
  All

Bay specific

• Restrictions:
  You must have access to the specified bay number.

• Example:
  OA-0018FE27577F> show server names
  show server names

Bay Server Name       Serial Number   Status   Power   UID
Partner
--- ----------------------------- --------------- -------- ------- ---
-------
1 First89123HostNameInILO USM64204B1  OK       On      Off
2 Integrity BL860c        CSJ0634214  OK       On      Off
3 [Absent]
4 [Absent]
5 [Subsumed]
6 [Subsumed]
7 YOUR-EYZCGYAYBB         USM62401EP  OK       On      On
8 [Absent]

Totals: 3 server blades installed, 3 powered on.
SHOW SERVER PORT MAP

- **Command:**
  
  SHOW SERVER PORT MAP {ALL | <bay number> [{, | - } <bay number>]}  

- **Description:**
  
  Displays the port mapping for the server specified by the bay number  

- **Access level/Bay level:**
  
  All
  
  Bay specific  

- **Restrictions:**
  
  - You must have access to the specified bay number.
  - This command is not applicable to storage blades.
  - Different sides of the server bay cannot be designated within the same range.

- **Example:**
  
  OA-0018FE27577F> SHOW SERVER PORT MAP ALL

<table>
<thead>
<tr>
<th>Mezz</th>
<th>Mezz</th>
<th>Device</th>
<th>Port</th>
<th>Status</th>
<th>Bay</th>
<th>Bay Port</th>
<th>Device ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slot</td>
<td>Device</td>
<td>Port</td>
<td>Status</td>
<td>Bay</td>
<td>Bay Port</td>
<td>Device ID</td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>-------</td>
<td>------</td>
<td>--------</td>
<td>---</td>
<td>--------</td>
<td>-----------</td>
<td></td>
</tr>
<tr>
<td>----</td>
<td>------</td>
<td>------</td>
<td>--------</td>
<td>---</td>
<td>--------</td>
<td>-----------</td>
<td></td>
</tr>
<tr>
<td>1 Not Present</td>
<td>2 Not Present</td>
<td>3 Not Present</td>
<td>Embedded Ethernet</td>
<td>Port 1 OK</td>
<td>Bay 1</td>
<td>Port 5</td>
<td>00:19:BB:24:51:0C</td>
</tr>
<tr>
<td>iSCSI 1 OK</td>
<td>Bay 1</td>
<td>Port 5</td>
<td>00:19:BB:24:51:0D</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port 2 OK</td>
<td>Bay 1</td>
<td>Port 13</td>
<td>00:19:BB:24:51:24</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iSCSI 2 OK</td>
<td>Bay 1</td>
<td>Port 13</td>
<td>00:19:BB:24:51:25</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port 3 OK</td>
<td>Bay 1</td>
<td>Port 1</td>
<td>00:19:BB:21:ED:EF</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port 4 OK</td>
<td>Bay 1</td>
<td>Port 9</td>
<td>00:19:BB:21:ED:F0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

-------------------------------- Blade 002 --------------------------------

| 1 Not Present | 2 Not Present | 3 Not Present | Embedded Ethernet | Port 1 OK | Bay 1 | Port 6 | 00:19:BB:34:A1:5A |
| iSCSI 1 OK | Bay 1 | Port 6 | 00:19:BB:34:A1:5B |
| Port 2 OK | Bay 1 | Port 14 | 00:19:BB:34:91:FE |
| iSCSI 2 OK | Bay 1 | Port 14 | 00:19:BB:34:91:FF |
| Port 3 OK | Bay 1 | Port 2 | 00:19:BB:29:91:33 |
| Port 4 OK | Bay 1 | Port 10 | 00:19:BB:29:91:34 |

-------------------------------- Blade 003 --------------------------------

| 1 Not Present | 2 Not Present | 3 Not Present | Embedded Ethernet | Port 1 OK | Bay 1 | Port 6 | 00:19:BB:34:A1:5A |
| iSCSI 1 OK | Bay 1 | Port 6 | 00:19:BB:34:A1:5B |
| Port 2 OK | Bay 1 | Port 14 | 00:19:BB:34:91:FE |
| iSCSI 2 OK | Bay 1 | Port 14 | 00:19:BB:34:91:FF |
| Port 3 OK | Bay 1 | Port 2 | 00:19:BB:29:91:33 |
| Port 4 OK | Bay 1 | Port 10 | 00:19:BB:29:91:34 |

<absent>

-------------------------------- Blade 004 --------------------------------

| 1 Not Present | 2 Not Present | 3 Not Present | Embedded Ethernet | Port 1 OK | Bay 1 | Port 6 | 00:19:BB:34:A1:5A |
| iSCSI 1 OK | Bay 1 | Port 6 | 00:19:BB:34:A1:5B |
| Port 2 OK | Bay 1 | Port 14 | 00:19:BB:34:91:FE |
| iSCSI 2 OK | Bay 1 | Port 14 | 00:19:BB:34:91:FF |
| Port 3 OK | Bay 1 | Port 2 | 00:19:BB:29:91:33 |
| Port 4 OK | Bay 1 | Port 10 | 00:19:BB:29:91:34 |
SHOW SERVER POWERDELAY

- **Command:**
  
  SHOW SERVER POWERDELAY {ALL | <bay number> [ { - | , } <bay number> ] }

- **Description:**
  
  Displays the PowerDelay status for the specified server blade or range of server blades

- **Access level/Bay level:**
  
  All
  
  Bay specific

- **Restrictions:**
  
  - You must have access to the specified bay number.
  
  - Different sides of the server bay cannot be designated within the same range.

- **Example:**
  
  OA-0018FE27577F> SHOW SERVER POWERDELAY ALL

  Current PowerDelay Status: Not in Progress

<table>
<thead>
<tr>
<th>Bay</th>
<th>Device</th>
<th>PowerDelay State</th>
<th>Delay (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Absent</td>
<td>Disabled</td>
<td>0</td>
</tr>
<tr>
<td>1A</td>
<td>Absent</td>
<td>Disabled</td>
<td>0</td>
</tr>
<tr>
<td>1B</td>
<td>Absent</td>
<td>Disabled</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>Subsumed</td>
<td>Disabled</td>
<td>0</td>
</tr>
<tr>
<td>2A</td>
<td>ProLiant BL2x220c G5</td>
<td>Disabled</td>
<td>0</td>
</tr>
<tr>
<td>2B</td>
<td>ProLiant BL2x220c G5</td>
<td>Disabled</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>Absent</td>
<td>Disabled</td>
<td>0</td>
</tr>
<tr>
<td>3A</td>
<td>Absent</td>
<td>Disabled</td>
<td>0</td>
</tr>
<tr>
<td>3B</td>
<td>Absent</td>
<td>Disabled</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>Absent</td>
<td>Disabled</td>
<td>0</td>
</tr>
<tr>
<td>4A</td>
<td>Absent</td>
<td>Disabled</td>
<td>0</td>
</tr>
<tr>
<td>4B</td>
<td>Absent</td>
<td>Disabled</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>Absent</td>
<td>Disabled</td>
<td>0</td>
</tr>
<tr>
<td>5A</td>
<td>Absent</td>
<td>Disabled</td>
<td>0</td>
</tr>
</tbody>
</table>
SHOW SERVER STATUS

- **Command:**
  SHOW SERVER STATUS {ALL | <bay number> [{ , | - } <bay number>]} |

- **Description:**
  Displays the following settings of server blade:
  - Power (OK or off)
  - Health (OK, CPU failure, or power module failure)
  - Thermal (OK, warm, caution, or critical)
  - UID LED

  If the power management controller is outdated or is in a lockup condition, a power management controller error appears.

- **Access level/Bay level:**
  All
  Bay specific

- **Restrictions:**
  - You must have access to the specified bay number.
  - Different sides of the server bay cannot be designated within the same range.

- **Example:**
  OA-0018FE27577F> show server status all
  Blade #1 Status:
  Power: On
  Current Wattage used: 212
  Health: OK
  Unit Identification LED: Off
  Diagnostic Status:
  - Internal Data OK
  - Management Processor OK
  - I/O Configuration OK
  - Power OK
  - Cooling OK
  - Location OK
  - Device Failure OK
  - Device Degraded OK
  - iLO Network OK

  Blade #2 Status:
  Power: On
  Current Wattage used: 360
Internal Health: OK
System Health: Degraded
Unit Identification LED: Off
Diagnostic Status:
  Internal Data        OK
  Management Processor OK
  I/O Configuration    OK
  Power                OK
  Cooling              OK
  Location             OK
  Device Failure       OK
  Device Degraded      OK

Blade #3 Status:
  Power: No Server Blade Installed

Blade #4 Status:
  Power: No Server Blade Installed

Blade #5 Status:
  Server Blade Type: Bay Subsumed

Blade #6 Status:
  Server Blade Type: Bay Subsumed

Blade #7 Status:
  Power: On
  Current Wattage used: 153
  Health: Degraded
  Unit Identification LED: On
  Diagnostic Status:
    Internal Data        OK
    Management Processor OK
    I/O Configuration    OK
    Power                OK
    Cooling              OK
    Location             OK
    Device Failure       OK
    Device Degraded      Failed
    iLO Network          OK
    IML Reported Main Memory Errors
      Uncorrectable Memory Error
        Processor 1, Memory Module 2
      Corrected Memory Error threshold exceeded
        Processor 1, Memory Module 2

• Example of Power Management Controller Error:
  OA-00215AB0DAF1> show server status 12

Blade #12 Status:
  Power: On
  Current Wattage used: 143
  Health: Other Unit Identification
  LED: Off Virtual
  Fan: 27%
  Diagnostic Status:
    Internal Data        OK
    Management Processor OK
    I/O Configuration    OK
    Power                OK
    Cooling              OK
    Location             OK
    Device Failure       OK
    Device Degraded      OK
SHOW SERVER TEMP

- **Command:**
  SHOW SERVER TEMP {ALL | <bay number> [{, | - } <bay number>]}
## Blade management commands

### Locale

<table>
<thead>
<tr>
<th>Critical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
</tr>
<tr>
<td>----------</td>
</tr>
<tr>
<td>--------</td>
</tr>
<tr>
<td>System Zone</td>
</tr>
<tr>
<td>CPU Zone</td>
</tr>
<tr>
<td>CPU 1</td>
</tr>
<tr>
<td>CPU 1</td>
</tr>
<tr>
<td>CPU Zone</td>
</tr>
<tr>
<td>CPU 2</td>
</tr>
<tr>
<td>CPU 2</td>
</tr>
<tr>
<td>Memory Zone</td>
</tr>
<tr>
<td>Ambient Zone</td>
</tr>
</tbody>
</table>

Virtual Fan: 25%

Device Bay #5 Temperature Information
Server Blade Type: Bay Subsumed

Device Bay #6 Temperature Information
Server Blade Type: Bay Subsumed

Device Bay #7 Temperature Information
No Server Blade Installed

Device Bay #8 Temperature Information
No Server Blade Installed

### SHOW SYSLOG SERVER

- **Command:**
  
  SHOW SYSLOG SERVER { All | <bay number> [{ ,| - } <bay number>]

- **Description:**
  Displays the syslog for the specified server blade

- **Access level/Bay level:**
  All
  Bay specific

- **Restrictions:**
  - You must have access to the specified bay number.
  - This command is not applicable to HP Integrity server blades.

- **Example:**
  
  OA-0018FE27577F> show syslog server 7
  Retrieving Server syslog(s) ...

  Server 7 Syslog:
  <EVENT_LOG DESCRIPTION="Integrated Management Log">
  <EVENT
    SEVERITY="Informational"
    CLASS="Rack Infrastructure"
    LAST_UPDATE="10/07/2007 23:51"
    INITIAL_UPDATE="10/07/2007 23:51"
    COUNT="1"
UNASSIGN SERVER

- **Command:**
  
  UNASSIGN SERVER {ALL | <bay number> [{, | - } <bay number>]} {"<user name>" | LDAP GROUP "<LDAP group name>"}

- **Description:**
  
  Removes specified servers from control of the user or group to which they are currently assigned

- **Access level/Bay level:**
  
  OA administrator
• **Restrictions:**
  None
Interconnect management commands

ASSIGN INTERCONNECT

- **Command:**
  
  ASSIGN INTERCONNECT {ALL | <bay number> [{ , | - } <bay number>]} {"<user name | LDAP GROUP <LDAP group name>"}

- **Description:**
  
  Assigns interconnects specified to an existing user or group

- **Access level/Bay level:**
  
  OA administrator

- **Restrictions:**
  
  None

CLEAR INTERCONNECT SESSION

- **Command:**
  
  CLEAR INTERCONNECT SESSION <bay number>

- **Description:**
  
  Terminates a serial console session of a user on an interconnect. The termination is not graceful and the user loses any unsaved work.

- **Access level/Bay level:**
  
  Administrator, operator

  Bay specific

- **Restrictions:**
  
  You must have explicit access to a bay given by the `ASSIGN INTERCONNECT` command.

CONNECT INTERCONNECT

- **Command:**
  
  CONNECT INTERCONNECT <bay number>

- **Description:**
  
  Connects the user to the serial console of the interconnect present in the interconnect module bay

- **Access level/Bay level:**
  
  All

  Bay specific

- **Restrictions:**
You must have explicit access to a bay given by the ASSIGN INTERCONNECT command.

**POWEROFF INTERCONNECT**

- **Command:**
  
  \[
  \text{POWEROFF INTERCONNECT} \{\text{ALL} \mid \text{<bay number>} \{ - \mid , \} \text{<bay number>}\}\]

- **Description:**
  
  Sends a request to power off the interconnect module

- **Access level/Bay level:**
  
  Administrator, operator
  
  Bay specific

- **Restrictions:**
  
  You must have explicit access to a bay given by the ASSIGN INTERCONNECT command.

**POWERON INTERCONNECT**

- **Command:**
  
  \[
  \text{POWERON INTERCONNECT} \{\text{ALL} \mid \text{<bay number>} \{ - \mid , \} \text{<bay number>}\}\]

- **Description:**
  
  Powers on the specified interconnect

- **Access level/Bay level:**
  
  Administrator, operator
  
  Bay specific

- **Restrictions:**
  
  You must have explicit access to a bay given by the ASSIGN INTERCONNECT command.

**RESTART INTERCONNECT**

- **Command:**
  
  \[
  \text{RESTART INTERCONNECT} \text{<bay number>}\]

- **Description:**
  
  Resets the interconnect tray in the specified bay

- **Access level/Bay level:**
  
  Administrator, operator
  
  Bay specific

- **Restrictions:**
  
  You must have explicit access to a bay given by the ASSIGN INTERCONNECT command.
SET INTERCONNECT ADMIN_PASSWORD FACTORY

- **Command:**
  SET INTERCONNECT ADMIN_PASSWORD FACTORY [<bay number>]

- **Description:**
  Causes the interconnect to change the Administrator password to the factory default. When you issue the command, you are prompted to confirm that this is your intention. To proceed with the change, answer YES. Upon successful execution of the command, the following message is logged to the Onboard Administrator syslog:
  
  OA: Interconnect module x Admin password has been reset by user Administrator.

  If the interconnect does not support the command, the Onboard Administrator displays the following message:
  
  This command is not supported by the interconnect.

- **Access level/Bay level:**
  Administrator
  Bay specific

- **Restrictions:**
  You must have access to the specified bay number.

SET INTERCONNECT FACTORY

- **Command:**
  SET INTERCONNECT FACTORY [<bay number>]

- **Description:**
  - Causes the interconnect to perform a factory reset, restoring all settings to their factory defaults.
  - Causes the Administrator password to be reset to the default factory password.
  - All configuration data and connections will be lost. You are prompted to confirm that you want to restore factory settings. To proceed with the change, answer YES. Upon successful execution of the command, the following message is logged to the Onboard Administrator syslog:
    
    OA: Interconnect module x has been Factory Reset by user Administrator.

  **IMPORTANT:** Before resetting factory defaults, save your configuration.

  - If the interconnect does not support the command, the Onboard Administrator displays the following message:
    
    This command is not supported by the interconnect.

- **Access level/Bay level:**
  Administrator
  Bay specific
Restrictions:
You must have access to the specified bay number.

SET INTERCONNECT POWERDELAY

Command:
SET INTERCONNECT POWERDELAY {ALL | <bay number> [{ - | , } <bay number>]}
{number of seconds to delay power | NOPOWERON}

Description:
Sets the PowerDelay status for the specified interconnect or range of interconnects. If the delay is zero, the delay has no effect on the device. If the delay is NOPOWERON, the device cannot power on until all devices have completed their delays.

Access level/Bay level:
Administrator
Bay specific

Restrictions:
You must have access to the specified bay number.

SET INTERCONNECT UID

Command:
SET INTERCONNECT UID {ALL | <bay number> [{ , | - } <bay number>]} {ON | OFF}

Description:
Turns an interconnect UID on or off

Access level/Bay level:
All
Bay specific

Restrictions:
You must have explicit access to a bay given by the ASSIGN INTERCONNECT command.

SHOW INTERCONNECT

Command:
SHOW INTERCONNECT {INFO | LIST [IPV6] | PORT MAP | POWERDELAY | SESSIONS | STATUS} [ALL | <bay number> | <bay number>-<bay number>]

Description:
- Displays the following information, depending on the keyword specified:
  - Interconnect type
  - IPv4 information
  - IPv6 information
  - Manufacturer name
— Product name
— Product part number
— Product version
— Product serial number
— Asset tag
— VLAN ID

- INTERCONNECT STATUS displays status information, UID state, and health state for the specified interconnects.
- INTERCONNECT PORT MAP displays port mapping information for the specified interconnects.
- INTERCONNECT SESSIONS shows which users, if any, have serial console sessions in progress for each interconnect.
- INTERCONNECT POWERDELAY shows the status and delay times for the specified interconnects.
- See also the SHOW INTERCONNECT INFO (on page 192) and SHOW INTERCONNECT LIST (on page 194) commands.

- **Access level/Bay level:**
  - All
  - Bay specific

- **Restrictions:**
  You must have explicit access to a bay given by the ASSIGN INTERCONNECT command.

- **Example:**
  OA-0018FE27577F> show interconnect info 1
  show interconnect info all

1. Ethernet
   Product Name: HP VC FlexFabric 10Gb/24-Port Module
   Width: Single
   URL to Management interface: http://172.16.1.70/
   In-Band IPv4 Address: 172.16.1.70
   User Assigned Name:
   Part Number: 571956-B21
   Spare Part Number: [Unknown]
   Serial Number: TW29460027
   Temperature Sensor: Present
   JS2 Connector: Absent
   Internal Ethernet Interface to OA: Present
   Internal Ethernet Route to OA: Enabled
   Internal Serial Interface to OA: Present
   Internal Serial Route to OA: Enabled
   Serial Port Baud Rate: 115200
   External Serial Port Interface: Absent
   External Ethernet Interface: Absent
   Manufacturer: HP
   Firmware Version: 4.10
SHOW INTERCONNECT INFO

- **Command:**
  
  SHOW INTERCONNECT INFO {PORT MAP | POWERDELAY | SESSIONS | STATUS} [ALL | <bay number> | <bay number>-<bay number>]

- **Description:**
  
  Displays:
  
  - Interconnect type
  - IPv4 information
  - IPv6 information
  - Manufacturer name
  - Product name
  - Product part number
  - Product version
  - Product serial number
  - Asset tag
  - VLAN ID

- **Access level/Bay level:**
  
  All
  
  Bay specific

- **Restrictions:**
  
  You must have explicit access to a bay. Access is given by the command ASSIGN INTERCONNECT (on page 187).

- **Example:**
  
  OA-0018FE27577F> show interconnect info all
  
  show interconnect info all

  1. Ethernet

     Product Name: HP VC Flex-10 Enet Module
     Width: Single
     URL to Management interface: http://111.22.3.444/
     In-Band IPv4 Address: 111.22.1.149
     User Assigned Name:
     Part Number: 455880-B21
     Spare Part Number: 456095-001
     Serial Number: TW2931005D
     Temperature Sensor: Present
     JS2 Connector: Absent
     Internal Ethernet Interface to OA: Present
     Internal Ethernet Route to OA: Enabled
     Internal Serial Interface to OA: Present
     Internal Serial Route to OA: Enabled
     Serial Port Baud Rate: 115200
     External Serial Port Interface: Absent
     External Ethernet Interface: Absent
     Manufacturer: HP
     Firmware Version: 4.10
VLAN ID: 1

IPv6 Information:
LL Address: fe80::223:aaaa:bbbb:9c4e/64
LL URL: http://[fe80::223:aaaa:bbbb:9c4e]
SLAAC Address: 1000::223:aaaa:bbbb:9c4e/64
SLAAC URL: http://[1000::223:aaaa:bbbb:9c4e]
DHCPv6 Address: 1000::1122:3344:5566:b91a/64
DHCPv6 URL: http://[1000::1122:3344:5566:b91a]

2. Ethernet
Product Name: HP VC Flex-10 Enet Module
Width: Single
URL to Management interface: http://111.22.3.555/
In-Band IPv4 Address: 111.22.2.156
User Assigned Name:
Part Number: 455880-B21
Spare Part Number: 456095-001
Serial Number: TW28420199
Temperature Sensor: Present
JS2 Connector: Absent
Internal Ethernet Interface to OA: Present
Internal Ethernet Route to OA: Enabled
Internal Serial Interface to OA: Present
Internal Serial Route to OA: Enabled
Serial Port Baud Rate: 115200
External Serial Port Interface: Absent
External Ethernet Interface: Absent
Manufacturer: HP
Firmware Version: 4.10
VLAN ID: 1
IPv6 Information:
LL Address: fe80::222:3333:4444:16d8/64
LL URL: http://[fe80::222:3333:4444:16d8]
SLAAC Address: 1000::222:3333:4444:16d8/64
SLAAC URL: http://[1000::222:3333:4444:16d8]
DHCPv6 Address: 1000::9999:4444:14a:1e2/64
DHCPv6 URL: http://[1000::9999:4444:14a:1e2]

3. <absent>
4. <absent>
5. <absent>
6. <absent>
7. <absent>
8. Fibre Channel
Product Name: HP 4Gb VC-FC Module
Width: Single
URL to Management interface:
In-Band IPv4 Address: 0.0.0.0
User Assigned Name:
Part Number: 409513-B21
Spare Part Number: 410152-001
Serial Number: MXK743004L
Temperature Sensor: Present
JS2 Connector: Absent
Internal Ethernet Interface to OA: Present
Internal Ethernet Route to OA: Enabled
Internal Serial Interface to OA: Absent
SHOW INTERCONNECT LIST

- **Command:**
  
  SHOW INTERCONNECT LIST [IPV6]

- **Description:**
  
  - Displays the interconnect list.
  - Displays IPv4 information by default. To display IPv6 information, enter the IPV6 keyword.

- **Access level/Bay level:**

  All

  Bay specific

- **Restrictions:**

  You must have explicit access to a bay. Access is given by the command **ASSIGN INTERCONNECT** (on page 187).

- **Example:**

  OA-0018FE27577F> SHOW INTERCONNECT LIST

<table>
<thead>
<tr>
<th>Bay</th>
<th>Interconnect Type</th>
<th>Manufacturer</th>
<th>Power</th>
<th>Health</th>
<th>UID</th>
<th>Management IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ethernet</td>
<td>HP</td>
<td>On</td>
<td>OK</td>
<td>Off</td>
<td>111.22.1.149</td>
</tr>
<tr>
<td>2</td>
<td>[Absent]</td>
<td>HP</td>
<td>On</td>
<td>OK</td>
<td>Off</td>
<td>111.22.2.156</td>
</tr>
<tr>
<td>3</td>
<td>[Absent]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>[Absent]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>[Absent]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>[Absent]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>[Absent]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Fibre Channel</td>
<td>HP</td>
<td>On</td>
<td>OK</td>
<td>Off</td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>

  Totals: 3 interconnect modules installed, 3 powered on.

  OA-0018FE27577F> SHOW INTERCONNECT LIST IPV6

<table>
<thead>
<tr>
<th>Bay</th>
<th>Interconnect Type</th>
<th>Power</th>
<th>Management IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ethernet</td>
<td>On</td>
<td>fe80::2222:3333:4444:100:LL</td>
</tr>
<tr>
<td>2</td>
<td>[Absent]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>[Absent]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>[Absent]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>[Absent]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

DHCPv6
Totals: 2 interconnect modules installed, 2 powered on.

**SHOW INTERCONNECT PORT MAP**

- **Command:**
  
  SHOW INTERCONNECT PORT MAP {ALL | <bay number> | <bay number>-<bay number>}

- **Description:**
  
  Displays the port mapping for the interconnect specified by the bay number

- **Access level/Bay level:**
  
  All
  
  Bay specific

- **Restrictions:**
  
  You must have explicit access to a bay given by the ASSIGN INTERCONNECT command.

- **Example:**

  OA-0018FE27577F> SHOW INTERCONNECT PORT MAP ALL

  1: Cisco Catalyst Blade Switch 3120X for HP w/ IP Base

  Type: Ethernet

  Width: Single

  Status: OK

<table>
<thead>
<tr>
<th>Port</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
</tr>
</tbody>
</table>
  
  1

  2. <absent>
  3. <absent>
  4. <absent>

**SHOW INTERCONNECT POWERDELAY**

- **Command:**

  SHOW INTERCONNECT POWERDELAY {ALL | <bay number> [{ - | , } <bay number>]]

- **Description:**

  Displays the PowerDelay status for the specified interconnects or range of interconnects

- **Access level/Bay level:**

  All

  Bay specific

- **Restrictions:**

  You must have access to the specified bay.
**Example:**
OA-0018FE27577F> SHOW INTERCONNECT POWERDELAY ALL
Current PowerDelay Status: Not in Progress

<table>
<thead>
<tr>
<th>Bay</th>
<th>Device</th>
<th>PowerDelay State</th>
<th>Delay (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Cisco Catalyst Blade Switch 3120</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Absent</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Absent</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Absent</td>
<td>Disabled</td>
<td></td>
</tr>
</tbody>
</table>

**SHOW INTERCONNECT SESSIONS**

- **Command:**
  
  SHOW INTERCONNECT SESSIONS

- **Description:**
  Displays which users have serial console sessions in progress for each interconnect

- **Access level/Bay level:**
  
  OA administrator, OA operator

  Bay specific

- **Restrictions:**
  
  You must have access to the specified bay.

- **Example:**
  
  OA-0018FE27577F> SHOW INTERCONNECT SESSION
  Interconnect Bay  User
  ------------------  --------------
  No Interconnect remote console sessions were detected.

**SHOW INTERCONNECT STATUS**

- **Command:**
  
  SHOW INTERCONNECT STATUS {ALL | <bay number> | <bay number>-<bay number>}

- **Description:**
  Displays interconnect status information.

- **Access level/Bay level:**
  
  All

  Bay specific

- **Restrictions:**
  
  You must have explicit access to a bay given by the ASSIGN INTERCONNECT command.

- **Example:**
  
  OA-0018FE27577F> SHOW INTERCONNECT STATUS ALL
  Interconnect Module #1 Status:
  Status : OK
  Thermal: OK
  CPU Fault: OK
  Health LED: OK
  UID: Off
Powered: On

Diagnostic Status:
- Internal Data: OK
- Management Processor: OK
- Thermal Warning: OK
- Thermal Danger: OK
- I/O Configuration: OK
- Device Failure: OK
- Device Degraded: OK

Interconnect Module #2 Status:
- Interconnect Module Type: No Interconnect Module Installed

Interconnect Module #3 Status:
- Interconnect Module Type: No Interconnect Module Installed

Interconnect Module #4 Status:
- Interconnect Module Type: No Interconnect Module Installed
Active Health System commands

ENABLE ACTIVE HEALTH SYSTEM

- **Command:**
  
  `ENABLE ACTIVE_HEALTH_SYSTEM`

- **Description:**
  Enables logging of inventory and health status for shared infrastructure items such as fans and power supplies to the blades that depend upon them.

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  None

DISABLE ACTIVE HEALTH SYSTEM

- **Command:**
  
  `DISABLE ACTIVE_HEALTH_SYSTEM`

- **Description:**
  Disables logging of inventory and health status for shared infrastructure items such as fans and power supplies to the blades that depend upon them.

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  None
Enclosure DVD commands

SET SERVER DVD

- Command:
  
  SET SERVER DVD {CONNECT | DISCONNECT} [USB://url] {ALL | <bay number> [{ , | - } <bay number>]}

- Description:
  
  Connects or disconnects the specified server or range of servers from the enclosure DVD drive. The DISCONNECT argument detaches any URL in addition to the enclosure DVD. USB://url is an optional parameter that matches the URL to an .iso file displayed by the SHOW USBKEY command.

- Access level/Bay level:
  
  Administrator, operator
  
  Bay specific

- Restrictions:
  
  You must have access to the specified bay number.

SHOW SERVER DVD

- Command:
  
  SHOW SERVER DVD {ALL | <bay number> [{ , | - } <bay number>]}

- Description:
  
  Displays the DVD connection status for the specified server or range of servers

- Access level/Bay level
  
  All
  
  Bay specific

- Restrictions:
  
  - You must have access to the specified bay number.
  - Different sides of the server bay cannot be designated within the same range.

- Example:

  OA-0018FE27577F> SHOW SERVER DVD ALL
  
  DVD Drive: Present
  DVD Media: Present
  Server DVD connections:
  Bay Connected Device or image URL
  --- ----------- ---------------------------------------
  1 - [Bay empty]
  2A No
  2B No
  3 - [Bay empty]
  4 - [Bay empty]
<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>[Bay empty]</td>
</tr>
<tr>
<td>6</td>
<td>[Bay empty]</td>
</tr>
<tr>
<td>7</td>
<td>No</td>
</tr>
<tr>
<td>8</td>
<td>[Non-server blade]</td>
</tr>
</tbody>
</table>
Remote syslog commands

DISABLE SYSLOG REMOTE

- **Command:**
  
  `DISABLE SYSLOG REMOTE`

- **Description:**
  
  Disables remote system logging

- **Access level/Bay level:**
  
  OA administrator, OA operator

- **Restrictions:**
  
  To perform this command, you must be an operator or administrator with OA permission.

ENABLE SYSLOG REMOTE

- **Command:**
  
  `ENABLE SYSLOG REMOTE`

- **Description:**
  
  Enables remote system logging

- **Access level/Bay level:**
  
  OA administrator, OA operator

- **Restrictions:**
  
  To perform this command, you must be an operator or administrator with OA permission.

SET REMOTE SYSLOG PORT

- **Command:**
  
  `SET REMOTE SYSLOG PORT <port>`

- **Description:**
  
  Sets the IP port number for remote system log. Setting the remote port is optional. If the remote port is not set, then the default UDP port 514 is used to send system log messages.

- **Access level/Bay level:**
  
  OA administrator, OA operator

- **Restrictions:**
  
  The remote port must be an integer between 1 and 65535 inclusive.
SET REMOTE SYSLOG SERVER

- **Command:**
  
  `SET REMOTE SYSLOG SERVER {<IPv4/IPv6> | <dns name>}`

- **Description:**
  
  Sets the IP address or DNS name for remote system log messages

- **Access level/Bay level:**
  
  OA administrator, OA operator

- **Restrictions:**
  
  None

SHOW SYSLOG SETTINGS

- **Command:**
  
  `SHOW SYSLOG SETTINGS`

- **Description:**
  
  Displays the remote syslog settings for the Onboard Administrator

- **Access level/Bay level:**
  
  Operator, Administrator

- **Restrictions:**
  
  You must have OA permission to perform this command.

- **Example:**
  
  `OA-0018FE27577F> SHOW SYSLOG SETTINGS`
  
  Remote log: Disabled
  Address: 
  Port: 514

TEST SYSLOG

- **Command:**
  
  `TEST SYSLOG`

- **Description:**
  
  Tests the remote system log settings by logging a test message to the syslog. The test message will also appear in the local OA administrator system log

- **Access level/Bay level:**
  
  Operator, Administrator

- **Restriction:**
  
  You must have OA permission to perform this command.
Remote syslog example

The remote syslog consists of a date and time stamp, the Onboard Administrator IP address, text, and a priority number. The date and time stamp, and the text match the Onboard Administrator syslog entry.

Sep  9 16:00:28 10.128.126.204 OA: Remote system logging enabled to server 16.83.33.81, port 514 (priority 13)
USB support commands

DOWNLOAD CONFIG using USB key

- **Command:**
  
  `DOWNLOAD CONFIG <url>`

- **Description:**
  
  Downloads a saved configuration file from a specific IP host. The file is not checked for errors but is automatically executed in script mode. Supported protocols are HTTP, FTP, TFTP, and USB. Format the `<url>` as protocol://host/path/file. If your FTP server does not support anonymous connections, then you can specify a username and password by replacing the host part in the previous format with username:password@host. To execute a configuration script from a USB key, use usb://<directory name>/<script file name>.

- **Access level/Bay level:**
  
  OA administrator

- **Restrictions:**
  
  - The file cannot change the Administrator account password.
  - The user password is not saved or restored by the `DOWNLOAD CONFIG` command.

SET SERVER DVD for USB key

- **Command:**
  
  `SET SERVER DVD {CONNECT | DISCONNECT} [USB://url] {ALL | <bay number> [{, | - } <bay number>]}`

- **Description:**
  
  Connects or disconnects the specified server or range of servers from the enclosure DVD drive. The DISCONNECT argument detaches any URL in addition to the enclosure DVD. USB://url is an optional parameter that matches the URL to an .iso file displayed by the `SHOW USB` command.

- **Access level/Bay level:**
  
  Administrator, operator

  Bay specific

- **Restrictions:**
  
  You must have access to the specified bay number.

SHOW USBKEY

- **Command:**
  
  `SHOW USBKEY`
• **Description:**
  Displays a list of Firmware images, configuration scripts, and ISO images present on the enclosure USB media

• **Access level/Bay level:**
  OA administrator, OA operator

• **Restriction:**
  None

• **Example:**
  OA-00215AB195CB> show usbkey

  ---
<table>
<thead>
<tr>
<th>Firmware Image Files</th>
<th>Image Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>usb://d1/hpoa225.bin</td>
<td>2.25</td>
</tr>
</tbody>
</table>

  ---
<table>
<thead>
<tr>
<th>Configuration Script Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>usb://d1/USE62317RY.cfg</td>
</tr>
</tbody>
</table>

  ---
<table>
<thead>
<tr>
<th>ISO Image Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>usb://d1/win2003sp4.iso</td>
</tr>
<tr>
<td>usb://d1/BB130.2008_0822.11.iso</td>
</tr>
<tr>
<td>usb://d1/HPSUMForce.iso</td>
</tr>
<tr>
<td>usb://d1/FW820.2008_0730.61.iso</td>
</tr>
</tbody>
</table>

**UPDATE IMAGE using USB key**

• **Command:**
  UPDATE IMAGE {{{FORCE} {<url> | FW_ISO}} | SYNC}

• **Description:**
  o The UPDATE IMAGE command downloads a new flash image from the network and uses it to update the Onboard Administrator firmware. If a redundant Onboard Administrator is present in the system, then this command flashes and validates its firmware before attempting to flash the active Onboard Administrator.

  o Supported protocols are HTTP, FTP, and TFTP.

  o The URL must be formatted as protocol://host/path/file.

  o The URL syntax for IPv6 addresses is protocol://[<ipv6 address>]/path/file.

  o If your FTP server does not support anonymous logins, a user name and password can be specified within the URL formatted as ftp://username:password@host/path/file.

  o Use FORCE to enable downgrading of firmware even if settings and passwords might be lost.

  o The UPDATE IMAGE SYNC command initiates a firmware sync of the Active and Standby Onboard Administrators.

  o For USB protocol, use SHOW USBKEY (on page 204).

• **Access level/Bay level:**
  OA administrator, OA operator
• Restrictions:
  o You cannot use the `FORCE` option for downgrade in FIPS Mode ON/DEBUG.
  o The maximum supported file size for USB keys formatted with FAT32 is 4GB. For SPP images greater than 4GB, use an ext2-formatted USB key. For information about formatting a USB key with an ext2 file system, see the *HP BladeSystem Onboard Administrator User Guide*.

⚠️ **CAUTION:** When a firmware upgrade is in process, do not disconnect or shut down the Onboard Administrator modules. Doing so could render the Onboard Administrator or server blade unusable.

**NOTE:** Updating the OA firmware from an OA version earlier than 3.50 to OA version 4.50 or later requires an intermediate update to OA 3.50 first, unless using the FW_ISO or SYNC arguments with the command. The intermediate OA 3.50 firmware can be downloaded from the HP Onboard Administrator website (http://h20564.www2.hp.com/hpsc/swd/public/detail?swItemId=MTX_00b278b5e9194e7ab0ab362d55).

### UPLOAD CONFIG using USB key

**• Command:**

`UPLOAD CONFIG {"<url>" | USB "<filename>"})`

**• Description:**

  o Uploads to the specified URL a script that duplicates the current runtime configuration.
  o Supported protocols are FTP, TFTP, and USB.
  o Format the URL as follows: protocol://host/path/file.
  o The URL syntax for IPv4 addresses is protocol://<ipv4 address>/path/file.
  o The URL syntax for IPv6 addresses is protocol://[<ipv6 address>]/path/file.
  o If your FTP server does not support anonymous connections, you can specify a user name and password in the format ftp://username:password@host/path/file.
  o To save an Onboard Administrator configuration file to a USB key, use the USB keyword and provide a file name.

**• Access level/Bay level:**

OA administrator

**• Restriction:**

The user password is not saved or restored by the *UPLOAD CONFIG* command.
VLAN commands

ADD VLAN

- **Command:**
  
  ADD VLAN <VLAN ID> ["<VLAN NAME>"]

- **Description:**
  Creates a VLAN ID and an optional VLAN NAME.

- **Access level/Bay level:**
  
  OA administrator, OA operator

- **Restrictions:**
  
  - The VLAN ID is an integer from 1 to 4094.
  - The VLAN Name is limited to 31 alphanumeric characters.

DISABLE VLAN

- **Command:**
  
  DISABLE VLAN

- **Description:**
  
  This command disables or turns off VLAN on the enclosure.

- **Access level/Bay level:**
  
  OA administrator, OA operator

- **Restrictions:**
  
  None

EDIT VLAN

- **Command:**
  
  EDIT VLAN <VLAN ID> ["<VLAN NAME>"]

- **Description:**
  
  Edits VLAN NAME (truncated to 31 alphanumeric characters) for the specified VLAN ID.

- **Access level/Bay level:**
  
  OA administrator, OA operator

- **Restrictions:**
  
  The VLAN Name is limited to 31 alphanumeric characters.
ENABLE VLAN

- **Command:**
  
  ENABLE VLAN

- **Description:**
  This command enables or turns on VLAN on the enclosure.

- **Access level/Bay level:**
  
  OA administrator, OA operator

- **Restrictions:**
  
  None

REMOVE VLAN

- **Command:**
  
  REMOVE VLAN <VLAN ID>

- **Description:**
  
  Removes a VLAN ID. All devices currently using that VLAN ID are moved to the default VLAN ID.

- **Access level/Bay level:**
  
  OA administrator, OA operator

- **Restrictions:**
  
  The user cannot remove the default VLAN ID.

SAVE VLAN

- **Command:**
  
  SAVE VLAN

- **Description:**
  
  Save VLAN configuration data to FLASH.

- **Access level/Bay level:**
  
  OA administrator, OA operator

- **Restrictions:**
  
  This command only applies to VLAN configuration data.

SET VLAN DEFAULT

- **Command:**
  
  SET VLAN DEFAULT <VLAN ID>

- **Description:**
  
  Sets or changes the default VLAN ID for the enclosure. Devices using the current default are reassigned to the new ID.
• **Access level/Bay level:**
  OA administrator, OA operator

• **Restrictions:**
  The VLAN ID is a value between 1 and 4094.

## SET VLAN FACTORY

• **Command:**
  SET VLAN FACTORY

• **Description:**
  Restores the VLAN settings to factory defaults. VLAN is disabled and all devices are grouped in VLAN ID 1. To execute the command, enter \texttt{YES} when asked if you are sure you want to restore VLAN settings to factory defaults.

• **Access level/Bay level:**
  OA administrator, OA operator

• **Restrictions:**
  None

## SET VLAN INTERCONNECT

• **Command:**
  \texttt{SET VLAN INTERCONNECT <VLAN\_ID> \{ ALL \| \textless bay\_number\textgreater \{ , \| - \} \textless bay\_number\textgreater \}}

• **Description:**
  Sets the VLAN ID for the specified interconnect or range of interconnects.

• **Access level/Bay level:**
  OA administrator, OA operator

• **Restrictions:**
  - You must create a VLAN ID using the \texttt{ADD VLAN} command, before using the \texttt{SET VLAN INTERCONNECT} command, or the command is rejected.
  - All Virtual Connects that belong to the same domain must be on the same VLAN.

## SET VLAN IPCONFIG

• **Command:**
  \texttt{SET VLAN IPCONFIG \{ DHCP \| STATIC \| SAVE \}}

• **Description:**
  Temporarily sets the OA VLAN ID and IP mode to DHCP or STATIC. The IP mode setting applies to the specific OA, and the VLAN ID setting applies to both OAs. If a VLAN ID does not exist, it is created. This command (typically used to test a new network setting) will undo its changes in 5 minutes. To permanently save the changes, issue the \texttt{SET VLAN IPCONFIG SAVE} command.
• **Access level/Bay level:**
  OA administrator, OA operator

• **Restrictions:**
  None

### SET VLAN IPCONFIG DHCP

**Command:**

```bash
SET VLAN IPCONFIG DHCP [<OA bay number>] <OA VLAN ID>
```

**Description:**

Temporarily sets the OA to DHCP mode and the specified VLAN ID (0 to 4094). Setting the VLAN ID number to 0 disables enclosure VLAN. Any other setting enables enclosure VLAN.

**Access level/Bay level:**

OA administrator, OA operator

**Restrictions:**

VLAN ID must be an integer between 0 and 4094.

### SET VLAN IPCONFIG SAVE

**Command:**

```bash
SET VLAN IPCONFIG SAVE
```

**Description:**

Saves the VLAN IPCONFIG changes to FLASH.

**Access level/Bay level:**

OA administrator, OA operator

**Restrictions:**

None

### SET VLAN IPCONFIG STATIC

**Command:**

```bash
SET VLAN IPCONFIG STATIC [<OA bay number>] <ip address> <netmask> [<gateway>] <OA VLAN ID>
```

**Description:**

Temporarily sets the OA to static IP mode and the specified VLAN ID (0 to 4094). Setting the VLAN ID number to 0 disables enclosure VLAN. Any other setting enables the enclosure VLAN.

**Access level/Bay level:**

OA administrator, OA operator

**Restrictions:**

VLAN ID must be an integer between 0 and 4094.
SET VLAN OA

- **Command:**
  
  SET VLAN OA <VLAN ID>

- **Description:**
  Sets or changes the VLAN ID of the Onboard Administrator. Loss of connectivity to the Onboard Administrator will occur if this is improperly set.

- **Access level/Bay level:**
  
  OA administrator, OA operator

- **Restrictions:**
  
  None

SET VLAN REVERT

- **Command:**
  
  SET VLAN REVERT <delay>

- **Description:**
  Reverts VLAN settings back to saved FLASH configuration data in <delay> seconds. Use a delay of 0 to cancel the command. Any newly issued revert command takes precedence over an outstanding one.

- **Access level/Bay level:**
  
  OA administrator, OA operator

- **Restrictions:**
  
  None

SET VLAN SERVER

- **Command:**
  
  SET VLAN SERVER <VLAN_ID> { ALL | <bay number> [{, | -} <bay number>] }

- **Description:**
  Sets the VLAN ID for the specified server or range of servers.

- **Access level/Bay level:**
  
  OA administrator, OA operator

- **Restrictions:**
  
  - You must create a VLAN ID using the ADD VLAN command, before using the SET VLAN SERVER command, or the command is rejected.
  - All multi-blade servers must be on the same VLAN.

SHOW VLAN

- **Command:**
SHOW VLAN

- **Description:**
  Shows VLAN settings.

- **Access level/Bay level:**
  OA administrator, OA operator, OA user

- **Restrictions:**
  None

- **Example:**
  OA-0018FE27577F> show vlan
  show vlan
  VLAN is enabled. OA VLAN ID = 1. Default VLAN ID (untagged) = 1.
  VLAN VLAN NAME
  ---- ---------
  1    Default
  Device Settings
  BAY VLAN
  --- ----
  1    1
  2    1
  3    1
  4    1
  5    1
  6    1
  7    1
  8    1
  Interconnect Settings
  BAY VLAN
  --- ----
  1    1
  2    1
  3    1
  4    1
ADD REMOTE_SUPPORT CERTIFICATE

- **Command:**
  
  ```
  ADD REMOTE_SUPPORT CERTIFICATE <end marker> <\n> <certificate> <\n> <end marker> <press enter>
  ```

- **Description:**
  Adds the specified HP Remote Support certificate to the Onboard Administrator. Certificates ensure that the Onboard Administrator sends information securely to the Insight Remote Control server. To add the certificate:
  a. Start with a string that does not appear within the certificate (the end marker).
  b. Insert a newline character by pressing `Enter`.
  c. Paste the certificate on the command line.
  d. Insert a newline character by pressing `Enter`.
  e. Insert the end marker.
  f. Issue the command by pressing `Enter`.

  Failure to give a proper end marker before and after the certificate might cause the interface to wait for the appropriate end marker indefinitely.

- **Access level/Bay level:**
  OA administrator

- **Restrictions**
  - Only one certificate may be added per command.
  - A maximum of 8 certificates can be added to the Onboard Administrator.
  - The maximum length of the certificate is 8192 characters.
  - This command is only available in script mode.
  - A valid certificate is required if connecting to an HP Insight Remote Support Hosting Device and the Onboard Administrator is operating in FIPS Mode.
  - When the Onboard Administrator is operating in FIPS Mode, certificates must have a minimum RSA key length of 2048 bits, and the signature hash algorithm must be SHA1, SHA-224, SHA-256, SHA-384, or SHA-512.

DOWNLOAD REMOTE_SUPPORT CERTIFICATE

- **Command:**
  
  ```
  DOWNLOAD REMOTE_SUPPORT CERTIFICATE "<url>"
  ```

- **Description:**
  
  The `DOWNLOAD REMOTE_SUPPORT CERTIFICATE` command is used to download a Remote Support certificate from a specified URL. This command is typically used when the certificate is hosted remotely and needs to be downloaded for use. The URL specifies the location of the certificate on a server.
Downloads the specified HP Remote Support certificate to the Onboard Administrator. The certificate ensures that the Onboard Administrator sends information securely to the Insight Remote Control server.

- Specify the URL where the certificate can be found.
- Supported protocols are HTTP, FTP, and TFTP.
- Format the URL as protocol://host/path/file.
- The URL syntax for IPv4 addresses is protocol://<ipv4 address>/path/file.
- The URL syntax for IPv6 addresses is protocol://[<ipv6 address>]/path/file.
- If your FTP server does not support anonymous connections, you can specify a user name and password in the format ftp://username:password@host/path/file.

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  - Only one certificate may be downloaded per command.
  - A maximum of 8 certificates can be downloaded to the Onboard Administrator.
  - A valid certificate is required if connecting to an HP Insight Remote Support Hosting Device and the Onboard Administrator is operating in FIPS Mode.
  - The maximum length of the certificate is 8192 characters.
  - When the Onboard Administrator is operating in FIPS Mode, certificates must have a minimum RSA key length of 2048 bits, and the signature hash algorithm must be SHA1, SHA-224, SHA-256, SHA-384, or SHA-512.

---

**ENABLE REMOTE_SUPPORT DIRECT**

- **Command:**
  
  ```
  ENABLE REMOTE_SUPPORT DIRECT {"<user-id>" "<password>"}
  ```

- **Description:**
  Registers the Onboard Administrator enclosure for the Insight Online direct connect (DIRECT mode) configuration option for HP Insight Remote Support, allowing the enclosure to communicate directly to HP without the need to set up an HP Insight Remote Support centralized Hosting Device in your local environment. For `<user-id>` and `<password>`, enter the HP Passport ID and password.

  After entering the command, you are asked to confirm that you agree to have Insight Remote Support send data to HP and that you agree to the terms and conditions of the HP Software License Agreement and the HP Insight Management Additional License Authorization (located at the HP website [http://www.hp.com/go/SWLicensing](http://www.hp.com/go/SWLicensing)). For information about the type of data collected by HP, see the *HP BladeSystem Onboard Administrator User Guide*.

  To confirm your agreement, answer *YES*. This completes the first of two steps of the registration process.

  **IMPORTANT:** This command completes step 1 of the registration process. To complete the process, you must perform step 2, which is to register at the Insight Online portal.

  To complete the second step of the registration process, register at the Insight Online portal:
  
  a. Navigate to the HP Insight Online website ([http://www.hp.com/go/insightonline](http://www.hp.com/go/insightonline)), and then log in with your HP Passport account credentials.
b. Follow the onscreen instructions in Insight Online, and provide your site, contact, and partner information so HP can deliver service for your enclosure. For detailed instructions, see the HP Insight Remote Support and Insight Online Setup Guide for HP ProLiant Servers and HP BladeSystem c-Class Enclosures.

After you complete these steps, confirm registration completion by using SET REMOTE_SUPPORT DIRECT ONLINE_REGISTRATION_COMPLETE (on page 217). To send a test event to confirm the connection between OA and Insight Remote Support, you can use TEST REMOTE_SUPPORT (on page 219).

If your enclosure uses a web proxy server to access the Internet, enter proxy information by using SET REMOTE_SUPPORT DIRECT PROXY (on page 217).

- **Access level/Bay level:**
  OA administrator

- **Restrictions**
  Version 4.01 or later of the Onboard Administrator firmware must be installed.

### ENABLE REMOTE_SUPPORT IRS

- **Command:**
  
  ```
  ENABLE REMOTE_SUPPORT IRS {"<hostname | IP address>" <port>}
  ```

- **Description:**
  Registers the Onboard Administrator enclosure for Insight Remote Support central connect (IRS mode), allowing the enclosure to communicate to HP through an HP Insight Remote Support centralized Hosting Device in your local environment. Specify the Hosting Device host name or IP address, and the port number.

  After registering, you can send a test event to confirm the connection between Onboard Administrator and Insight Remote Support by using TEST REMOTE_SUPPORT (on page 219).

- **Access level/Bay level:**
  OA administrator

- **Restrictions**
  - Insight Remote Support 7.0.5 or later must be installed and configured on the Insight Remote Support centralized Hosting Device.
  - Version 3.60 or later of the Onboard Administrator firmware must be installed.
  - A valid certificate is required if connecting to an HP Insight Remote Support Hosting Device and the Onboard Administrator is operating in FIPS Mode.

### ENABLE REMOTE_SUPPORT MAINTENANCE

- **Command:**
  
  ```
  ENABLE REMOTE_SUPPORT MAINTENANCE { MIN | HOUR | DAY | WEEK } <interval>
  ```

- **Description:**
  Enables and starts the Remote Support maintenance window for the time interval specified

- **Access level/Bay level:**
OA administrator

- **Restrictions:**
  Remote Support must be enabled before running `ENABLE REMOTE_SUPPORT MAINTENANCE`. This setting is not recorded when you run the `SHOW CONFIG` command.

**DISABLE REMOTE_SUPPORT**

- **Command:**
  `DISABLE REMOTE_SUPPORT`

- **Description:**
  Unregisters the Onboard Administrator from the Remote Support server

- **Access level/Bay level:**
  OA administrator

**DISABLE REMOTE_SUPPORT MAINTENANCE**

- **Command:**
  `DISABLE REMOTE_SUPPORT MAINTENANCE`

- **Description:**
  Disables the Remote Support maintenance window

- **Access level/Bay level:**
  OA administrator

**REMOVE REMOTE_SUPPORT CERTIFICATE**

- **Command:**
  `REMOVE REMOTE_SUPPORT CERTIFICATE "<certificate name>"`

- **Description:**
  Removes the Remote Support trust certificate corresponding to the SHA1 `<certificate name>`.

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  None

**SEND REMOTE_SUPPORT DATACOLLECTION**

- **Command:**
  `SEND REMOTE_SUPPORT DATACOLLECTION`

- **Description:**
  Sends a data collection to the remote server
• **Access level/Bay level:**
  OA administrator

• **Restrictions:**
  Remote Support must be enabled before sending a data collection. If the enclosure contains a large number of blades, the test might take several minutes. After the test is complete, the status is reflected in the `SHOW REMOTE_SUPPORT` command output.

---

### SET REMOTE_SUPPORT DIRECT ONLINE_REGISTRATION_COMPLETE

• **Command:**
  ```
  SET REMOTE_SUPPORT DIRECT ONLINE_REGISTRATION_COMPLETE
  ```

• **Description:**
  Upon entering this command, you are asked to confirm that you registered at the HP Insight Online website (http://www.hp.com/go/insightonline). This is the second of two steps to finish registering for Insight Remote Support through a direct connection to HP Insight Online. To confirm that you have completed this step, answer YES.

  To send a test event to confirm the connection between OA and Insight Remote Support, use the `TEST REMOTE_SUPPORT` (on page 219) command.

• **Access level/Bay level:**
  OA administrator

• **Restrictions**
  If your enclosure uses a web proxy server to access the Internet, enter proxy information with the `SET REMOTE_SUPPORT DIRECT PROXY` (on page 217) command. Proxy settings must be kept up to date to enable your c-Class enclosure to continue to send remote support data to HP.

---

### SET REMOTE_SUPPORT DIRECT PROXY

• **Command:**
  ```
  SET REMOTE_SUPPORT DIRECT PROXY {NONE | "<proxy server>" <proxy port> ["<proxy username>"] ["<proxy password>"]}
  ```

• **Description:**
  Sets Remote Support proxy settings required if the Onboard Administrator enclosure uses a proxy server to access the Internet.

• **Access level/Bay level:**
  OA administrator

• **Restrictions**
  Proxy settings must be kept up to date to enable your c-Class enclosure to continue to send remote support data to HP.
SHOW REMOTE_SUPPORT

- **Command:**
  
  SHOW REMOTE_SUPPORT

- **Description:**
  Displays Remote Support settings and information such as:
  - Remote Support status
  - Connection type: DIRECT or IRS (Insight Remote Support)
  - Online Registration status
  - Online Passport User ID, if connection type is DIRECT
  - Hosting Device name and port, if connection type is IRS (central)
  - Web Proxy Server
  - Data collection status

- **Access level/Bay level:**
  OA administrator

- **Example:**
  
  OA-E4115BECFBAB> show remote_support

  Status : Enabled
  Connection type : DIRECT
  Online Passport ID : oa_user
  Online Registration complete : Yes
  Web Proxy Server :
  Collection Interval(days) : 30
  Last successful registration : 2013-11-11T12:21:40 CST
  Last successful unregistration : 0000-00-00T00:00:00
  Last successful Data Collection : 2013-11-11T12:22:05 CST
  Last Data Collection transmission: 2013-11-11T12:22:05 CST
  Next scheduled Data Collection : 2013-12-11T12:25:18 CST
  Failed Data Collection attempts : 0
  Failed Service Event attempts : 0
  Maintenance Mode : Disabled

SHOW REMOTE_SUPPORT CERTIFICATE

- **Command:**
  
  SHOW REMOTE_SUPPORT CERTIFICATE

- **Description:**
  Displays the details of the Remote Support certificates that have been added.

- **Access level/Bay level:**
  OA administrator

- **Restrictions**
  None

- **Example:**
SHOW REMOTE_SUPPORT EVENTS

- **Command:**
  `SHOW REMOTE_SUPPORT EVENTS`

- **Description:**
  Displays Remote Support events that have been sent

- **Access level/Bay level:**
  OA administrator

- **Example:**
  OA-E4115BECFBAB> show remote_support events

<table>
<thead>
<tr>
<th>Id</th>
<th>Time</th>
<th>Event</th>
<th>Device</th>
<th>Serial Number</th>
<th>Perceived Submission Number</th>
<th>Bay</th>
<th>Severity</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>80965f29-7f7e-42ba-af8-8bd348c75bb</td>
<td>2013-11-11T12:23:09 CST Test</td>
<td>Enclosure ENC1234567</td>
<td>0</td>
<td>Info</td>
<td>OK</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b6cd7095-a561-4384-98b2-5e4474e2a2dc</td>
<td>2013-11-11T12:25:09 CST Test</td>
<td>Enclosure ENC1234567</td>
<td>0</td>
<td>Info</td>
<td>OK</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>f7824402-6e46-4e02-b584-4c7a84b49504</td>
<td>2013-11-11T12:25:11 CST Test</td>
<td>Enclosure ENC1234567</td>
<td>0</td>
<td>Info</td>
<td>OK</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>d45e1b4c-fa23-4b7e-917d-f9d3857aedfb</td>
<td>2013-11-11T12:25:12 CST Test</td>
<td>Enclosure ENC1234567</td>
<td>0</td>
<td>Info</td>
<td>OK</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

TEST REMOTE_SUPPORT

- **Command:**
  `TEST REMOTE_SUPPORT`
**TEST REMOTE_SUPPORT**

- **Description:**
  Sends a test service alert

- **Access level/Bay level:**
  OA administrator

- **Restrictions:**
  Remote Support must be enabled before sending a test event. If the enclosure contains a large number of blades, the test might take several minutes. After the test has completed, the status is reflected in the `SHOW REMOTE_SUPPORT` command output.
Enclosure Dynamic Power Cap commands

SET ENCLOSURE POWER_CAP

- **Command:**
  
  SET ENCLOSURE POWER_CAP { <cap> [derated_circuit_capacity] <rated_circuit_capacity> ] | OFF }

- **Description:**
  
  Sets the Enclosure Dynamic Power Cap in watts AC. OFF disables the Enclosure Dynamic Power Cap. Average power cannot exceed cap or derated_circuit_capacity. Peak power cannot exceed rated_circuit_capacity. For example, suppose the PDU powering the enclosure has a rated capacity of 30 amps. In North America and Japan, the standard de-rating ratio is 80%, so the PDU has a derated capacity of 24 amps (0.80 * 30). At 208 volts, the Rated Circuit Capacity would be entered as 6240 watts (30 * 208), and the Derated Circuit Capacity would be entered as 4992 watts (24 * 208). When specifying only cap, the other values are calculated using the standard de-rating ratio for North America. Therefore derated_circuit_capacity is equal to cap and rated_circuit_capacity is equal to 1.25 * cap. The Enclosure Dynamic Power Cap and Derated Circuit Capacity can be specified as any value in the allowable range. The Derated Circuit Capacity must be at least as large as the Enclosure Dynamic Power Cap and no larger than the Rated Circuit Capacity. The Enclosure Dynamic Power Cap can be used to limit enclosure power consumption based on a cooling constraint that might be lower than the Derated Circuit Capacity.

- **Access level/Bay level:**
  
  OA administrator, OA operator

- **Restrictions:**
  
  o A redundant Onboard Administrator is required.
  o The Power Cap must be in the range displayed by the command `SHOW ENCLOSURE POWER_CAP`.
  o In scripts, if both `SET POWER LIMIT` and `SET ENCLOSURE POWER_CAP` are set to non-zero values, whichever command is used last takes precedence.

SET ENCLOSURE POWER_CAP_BAYS_TO_EXCLUDE

- **Command:**
  
  SET ENCLOSURE POWER_CAP_BAYS_TO_EXCLUDE [NONE | <bay number> {[ , | - ] <bay number> }]

- **Description:**
  
  Specifies bays to omit from Enclosure Dynamic Power Cap. Blades in omitted bays are treated as unmanaged components of the system: They receive a maximum power allocation even when the power is not being consumed, raising the minimum Enclosure Dynamic Power Cap value that can be applied to the enclosure. Any blades in bays not specified are managed.
If you have previously specified bays to exclude, using this command again replaces that specification rather than augmenting it.

- **Access level/Bay level:**
  OA administrator, OA operator

- **Restriction:**
  You can exclude no more than one fourth of the bays.

### SHOW ENCLOSURE POWER_CAP

- **Command:**
  SHOW ENCLOSURE POWER_CAP

- **Description:**
  Displays the current Enclosure Dynamic Power Cap in watts.

- **Access level/Bay level:**
  All

- **Restriction:**
  None

- **Example:**
  OA-0018FE27577> SHOW ENCLOSURE POWER_CAP

  Enclosure Dynamic Power Cap: Disabled
  Derated Circuit Capacity: Disabled
  Rated Circuit Capacity: Disabled
  Allowable Enclosure Dynamic Power Cap: 3123 - 7676 Watts AC
  Allowable Derated Circuit Capacity: 3123 - 7676 Watts AC
  Allowable Rated Circuit Capacity: 3428 - 7676 Watts AC

### SHOW ENCLOSURE POWER_CAP_BAYS_TO_EXCLUDE

- **Command:**
  SHOW ENCLOSURE POWER_CAP_BAYS_TO_EXCLUDE

- **Description:**
  Displays the bays in the enclosure that are exempt from the Enclosure Dynamic Power Cap.

- **Access level/Bay level:**
  All

- **Restriction:**
  None

- **Example:**
  OA-0018FE27577F> show enclosure power_cap_bays_to_exclude

  Bays opted out: None
Event notifications

Enclosure event notifications

Enclosure events produce screen messages with the `show events` option enabled. If you are directly affected by an event, a message is produced whether the `show events` option is enabled or disabled.

Event messages include the device affected, the device name, and the date and time of the event. Some examples of event messages are:

- The enclosure is in a degraded state.
- Blade X has experienced a failure.
- The temperature on Blade X has exceeded the failed threshold.
- Fan X has experienced a failure.
- The power supplies are no longer redundant.
- Power supply X is in a degraded state.
- The enclosure temperature has exceeded the degraded threshold.

Command line event notifications

When the `SET DISPLAY EVENTS` option is turned on, the terminal interface displays error, warning, and status messages, depending on the behavior of the enclosure and components.

The syntax for these messages are:

- `<error>`—Description of error
- `<warning>`—Description of warning
- `<status>`—Description of status

The following table lists causes of the error, warning, or status events that appear.

<table>
<thead>
<tr>
<th>Event</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bay Event</td>
<td>A bay was assigned or unassigned from a group.</td>
</tr>
<tr>
<td>Blade Inserted</td>
<td>A blade was inserted into the enclosure.</td>
</tr>
<tr>
<td>Blade Thermal Status Changed</td>
<td>The thermal status of a blade changed.</td>
</tr>
<tr>
<td>Blade Removed</td>
<td>A blade was removed from the enclosure.</td>
</tr>
<tr>
<td>Blade Port Map Info</td>
<td>The port mapping information of a blade was updated.</td>
</tr>
<tr>
<td>Enclosure Status Change</td>
<td>A change in status has occurred because of a change in the state of one or more hardware components or server readings.</td>
</tr>
<tr>
<td>Enclosure Name Change</td>
<td>The name of the enclosure was changed.</td>
</tr>
<tr>
<td>Event</td>
<td>Cause</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Fan Status Change</td>
<td>The status of a fan has changed.</td>
</tr>
<tr>
<td>Fan Inserted</td>
<td>A fan has been inserted.</td>
</tr>
<tr>
<td>Fan Removed</td>
<td>A fan has been removed.</td>
</tr>
<tr>
<td>Interconnect Inserted</td>
<td>An interconnect module was inserted into the enclosure.</td>
</tr>
<tr>
<td>Interconnect Thermal Status Changed</td>
<td>The thermal status of an interconnect module changed.</td>
</tr>
<tr>
<td>Interconnect Removed</td>
<td>An interconnect module was removed from the enclosure.</td>
</tr>
<tr>
<td>Interconnect Power Reset</td>
<td>The power of an interconnect module was reset.</td>
</tr>
<tr>
<td>Interconnect Port Map Info</td>
<td>The port mapping information of an interconnect module was updated.</td>
</tr>
<tr>
<td>LDAP Group Removed</td>
<td>A LDAP group was removed from the Onboard Administrator. If you are logged into the Onboard Administrator under this LDAP group, you are disconnected.</td>
</tr>
<tr>
<td>OA System Log Cleared</td>
<td>The Onboard Administrator system log was cleared.</td>
</tr>
<tr>
<td>OA Name Changed</td>
<td>The Onboard Administrator DNS name was changed.</td>
</tr>
<tr>
<td>OA Inserted</td>
<td>A redundant Onboard Administrator was inserted into the enclosure.</td>
</tr>
<tr>
<td>OA Removed</td>
<td>The redundant Onboard Administrator was removed from the enclosure.</td>
</tr>
<tr>
<td>OA Takeover</td>
<td>The redundant and active Onboard Administrators are switching roles. The Active Onboard Administrator reboots into Standby Mode and the redundant Onboard Administrator transitions to Active Mode.</td>
</tr>
<tr>
<td>Power Supply Status Change</td>
<td>The status of a power supply has changed.</td>
</tr>
<tr>
<td>Power Supply Inserted</td>
<td>A power supply has been inserted.</td>
</tr>
<tr>
<td>Power Supply Removed</td>
<td>A power supply has been removed.</td>
</tr>
<tr>
<td>Power Supply Redundancy Change</td>
<td>The power supplies are either now redundant or are no longer redundant.</td>
</tr>
<tr>
<td>Power Supply Overload</td>
<td>The power supplies are being asked to draw more current than they are able.</td>
</tr>
<tr>
<td>Restart Event</td>
<td>The Onboard Administrator is about to start.</td>
</tr>
<tr>
<td>Rack Name Change</td>
<td>The rack name stored on the enclosure was changed.</td>
</tr>
<tr>
<td>Rack Topology</td>
<td>Enclosures were connected or disconnected from the enclosure link.</td>
</tr>
<tr>
<td>Thermal Status Change</td>
<td>A thermal sensor has changed state.</td>
</tr>
<tr>
<td>User Removed</td>
<td>A user was removed from the Onboard Administrator. If you are logged in as this user, you are disconnected from the Onboard Administrator.</td>
</tr>
<tr>
<td>User Disabled</td>
<td>A user was disabled. If you are logged in as this user, you are disconnected from the Onboard Administrator.</td>
</tr>
<tr>
<td>Event</td>
<td>Cause</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User Rights</td>
<td>The privilege level of a user on the Onboard Administrator was changed. If you are logged in as this user, you are disconnected from the Onboard Administrator. You can log in again with your new privilege level.</td>
</tr>
</tbody>
</table>
Support and other resources

Before you contact HP

Be sure to have the following information available before you call HP:

- **Active Health System log (HP ProLiant Gen8 or later products)**
  Download and have available an Active Health System log for 7 days before the failure was detected. For more information, see the **HP iLO 4 User Guide** or **HP Intelligent Provisioning User Guide** on the HP website (http://www.hp.com/go/ilo/docs).

- **Onboard Administrator SHOW ALL report (for HP BladeSystem products only)**
  For more information on obtaining the Onboard Administrator SHOW ALL report, see the HP website (http://www.hp.com/go/OAlog).

- **Technical support registration number (if applicable)**
- **Product serial number**
- **Product model name and number**
- **Product identification number**
- **Applicable error messages**
- **Add-on boards or hardware**
- **Third-party hardware or software**
- **Operating system type and revision level**

HP contact information

For United States and worldwide contact information, see the Contact HP website (http://www.hp.com/go/assistance).

In the United States:

- To contact HP by phone, call 1-800-334-5144. For continuous quality improvement, calls may be recorded or monitored.

- If you have purchased a Care Pack (service upgrade), see the Support & Drivers website (http://www8.hp.com/us/en/support-drivers.html). If the problem cannot be resolved at the website, call 1-800-633-3600. For more information about Care Packs, see the HP website (http://pro-aq-sama.houston.hp.com/services/cache/10950-0-0-225-121.html).
### Additional information

<table>
<thead>
<tr>
<th>For the following...</th>
<th>Refer to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP Onboard Administrator documentation including user guides and release notes</td>
<td>HP Onboard Administrator Information Library (<a href="http://www.hp.com/support/oa/docs">http://www.hp.com/support/oa/docs</a>)</td>
</tr>
<tr>
<td>HP Onboard Administrator product information and additional resources, including</td>
<td>HP Onboard Administrator product website (<a href="http://www.hp.com/go/oa">http://www.hp.com/go/oa</a>)</td>
</tr>
<tr>
<td>links to QuickSpecs, user guides, release notes, white papers, and other documentation</td>
<td></td>
</tr>
<tr>
<td>HP Insight Management documentation</td>
<td>HP Insight Management Information Library (<a href="http://www.hp.com/go/insightmanagement/docs">http://www.hp.com/go/insightmanagement/docs</a>)</td>
</tr>
<tr>
<td>iLO Management Engine documentation</td>
<td>HP iLO Management Engine Information Library (<a href="http://www.hp.com/go/ilomgmtengine/docs">http://www.hp.com/go/ilomgmtengine/docs</a>)</td>
</tr>
</tbody>
</table>
## Time zone settings

### Universal time zone settings

**IMPORTANT:** Time zones must be entered exactly as they appear.

The following table provides the Universal time zone settings that are supported by the Onboard Administrator.

<table>
<thead>
<tr>
<th>Time Zone</th>
<th>UTC Offset</th>
<th>Time Zone Name</th>
<th>Zone Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>CET</td>
<td>0</td>
<td>Etc/GMT+2</td>
<td>UTC</td>
</tr>
<tr>
<td>CST6CDT</td>
<td>Etc/GMT-3</td>
<td>Etc/GMT+8</td>
<td>MST</td>
</tr>
<tr>
<td>EET</td>
<td>Etc/GMT+3</td>
<td>Etc/UCT</td>
<td>Navajo</td>
</tr>
<tr>
<td>EST</td>
<td>Etc/GMT-4</td>
<td>Etc/GMT+9</td>
<td>PST8PDT</td>
</tr>
<tr>
<td>EST5EDT</td>
<td>Etc/GMT+4</td>
<td>Etc/GMT+10</td>
<td>Factory</td>
</tr>
<tr>
<td>Etc/GMT5</td>
<td>Etc/GMT-5</td>
<td>Etc/GMT-11</td>
<td>Universal</td>
</tr>
<tr>
<td>Etc/GMT0</td>
<td>Etc/GMT+5</td>
<td>Etc/GMT+11</td>
<td>GMT+0</td>
</tr>
<tr>
<td>Etc/GMT-6</td>
<td>Etc/GMT+6</td>
<td>GMT+0</td>
<td>WET</td>
</tr>
<tr>
<td>Etc/GMT+0</td>
<td>Etc/GMT+6</td>
<td>GMT+0</td>
<td>W:SU</td>
</tr>
<tr>
<td>Etc/GMT+7</td>
<td>Etc/GMT+7</td>
<td>GMT+0</td>
<td>—</td>
</tr>
<tr>
<td>Etc/GMT+8</td>
<td>Etc/GMT+8</td>
<td>GMT+0</td>
<td>—</td>
</tr>
</tbody>
</table>

### Africa time zone settings

**IMPORTANT:** Time zones must be entered exactly as they appear.

The following table provides the African time zone settings that are supported by the Onboard Administrator.

<table>
<thead>
<tr>
<th>Africa/Abidjan</th>
<th>Africa/Ceuta</th>
<th>Africa/Kinshasa</th>
<th>Africa/Niamey</th>
</tr>
</thead>
<tbody>
<tr>
<td>Africa/Accra</td>
<td>Africa/Conakry</td>
<td>Africa/Lagos</td>
<td>Africa/Nouakchott</td>
</tr>
<tr>
<td>Africa/Addis_Ababa</td>
<td>Africa/Dakar</td>
<td>Africa/Libreville</td>
<td>Africa/Ouagadougou</td>
</tr>
<tr>
<td>Africa/Algiers</td>
<td>Africa/Dar_es_Salaam</td>
<td>Africa/Lome</td>
<td>Africa/Porto-Novo</td>
</tr>
<tr>
<td>Africa/Asmara</td>
<td>Africa/Djibouti</td>
<td>Africa/Luanda</td>
<td>Africa/Sao_Tome</td>
</tr>
<tr>
<td>Africa/Asmera</td>
<td>Africa/Douala</td>
<td>Africa/Lubumbashi</td>
<td>Africa/Timbuktu</td>
</tr>
<tr>
<td>Africa/Bamako</td>
<td>Africa/El_Aaiun</td>
<td>Africa/Lusaka</td>
<td>Africa/Tripoli</td>
</tr>
<tr>
<td>Africa/Bangui</td>
<td>Africa/Freetown</td>
<td>Africa/Malabo</td>
<td>Africa/Tunis</td>
</tr>
<tr>
<td>Africa/Banjul</td>
<td>Africa/Gaborone</td>
<td>Africa/Maputo</td>
<td>Africa/Windhoek</td>
</tr>
<tr>
<td>Africa/Bissau</td>
<td>Africa/Harare</td>
<td>Africa/Maseru</td>
<td>Egypt</td>
</tr>
<tr>
<td>Africa/Blantyre</td>
<td>Africa/Johannesburg</td>
<td>Africa/Mbabane</td>
<td>Libya</td>
</tr>
<tr>
<td>Africa/Brazzaville</td>
<td>Africa/Juba</td>
<td>Africa/Mogadishu</td>
<td>—</td>
</tr>
<tr>
<td>Africa/Bujumbura</td>
<td>Africa/Kampala</td>
<td>Africa/Monrovia</td>
<td>—</td>
</tr>
<tr>
<td>Africa/Cairo</td>
<td>Africa/Khartoum</td>
<td>Africa/Nairobi</td>
<td>—</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------------</td>
<td>-------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Africa/Casablanca</td>
<td>Africa/Kigali</td>
<td>Africa/Ndjamena</td>
<td>—</td>
</tr>
</tbody>
</table>

**Americas time zone settings**

**IMPORTANT:** Time zones must be entered exactly as they appear.

The following table provides the Americas time zone settings that are supported by the Onboard Administrator.

<table>
<thead>
<tr>
<th>America/Adak</th>
<th>America/Guatemala</th>
<th>America/Rainy_River</th>
</tr>
</thead>
<tbody>
<tr>
<td>America/Anchorage</td>
<td>America/Guayaquil</td>
<td>America/Rankin_Inlet</td>
</tr>
<tr>
<td>America/Anguilla</td>
<td>America/Guyana</td>
<td>America/Recife</td>
</tr>
<tr>
<td>America/Antigua</td>
<td>America/Halifax</td>
<td>America/Regina</td>
</tr>
<tr>
<td>America/Araquai</td>
<td>America/Havana</td>
<td>America/Resolute</td>
</tr>
<tr>
<td>America/Argentina/Buenos_Aires</td>
<td>America/Hermosillo</td>
<td>America/Rio_Branco</td>
</tr>
<tr>
<td>America/Argentina/Catamarca</td>
<td>America/Indiana/Indianapolis</td>
<td>America/Rosario</td>
</tr>
<tr>
<td>America/Argentina/ComodRivadavia</td>
<td>America/Indiana/Knox</td>
<td>America/Santa_Isabel</td>
</tr>
<tr>
<td>America/Argentina/Cordoba</td>
<td>America/Indiana/Marengo</td>
<td>America/Santarem</td>
</tr>
<tr>
<td>America/Argentina/Jujuy</td>
<td>America/Indiana/Petersburg</td>
<td>America/Santiago</td>
</tr>
<tr>
<td>America/Argentina/La_Rioja</td>
<td>America/Indiana/Tell_City</td>
<td>America/Santo_Domingo</td>
</tr>
<tr>
<td>America/Argentina/Mendoza</td>
<td>America/Indiana/Vevay</td>
<td>America/Sao_Paulo</td>
</tr>
<tr>
<td>America/Argentina/Rio_Gallegos</td>
<td>America/Indiana/Vincennes</td>
<td>America/Scoresbysund</td>
</tr>
<tr>
<td>America/Argentina/Salta</td>
<td>America/Indiana/Winamac</td>
<td>America/Shiprock</td>
</tr>
<tr>
<td>America/Argentina/San_Juan</td>
<td>America/Indianapolis</td>
<td>America/Sitka</td>
</tr>
<tr>
<td>America/Argentina/San_Luis</td>
<td>America/Inuvik</td>
<td>America/St_Barthelemy</td>
</tr>
<tr>
<td>America/Argentina/Tucuman</td>
<td>America/Iqaluit</td>
<td>America/St_Johns</td>
</tr>
<tr>
<td>America/Argentina/Ushuaia</td>
<td>America/Jamaica</td>
<td>America/St_Kitts</td>
</tr>
<tr>
<td>America/Aruba</td>
<td>America/Jujuy</td>
<td>America/St_Lucia</td>
</tr>
<tr>
<td>America/Asuncion</td>
<td>America/Juneau</td>
<td>America/St_Thomas</td>
</tr>
<tr>
<td>America/Atikokan</td>
<td>America/Kentucky/Louisville</td>
<td>America/St_Vincent</td>
</tr>
<tr>
<td>America/Atka</td>
<td>America/Kentucky/Monticello</td>
<td>America/Swift_Current</td>
</tr>
<tr>
<td>America/Bahia</td>
<td>America/Knox_IN</td>
<td>America/Tegucigalpa</td>
</tr>
<tr>
<td>America/Bahia_Banderas</td>
<td>America/Kralendijk</td>
<td>America/Thule</td>
</tr>
<tr>
<td>America/Barbados</td>
<td>America/La_Paz</td>
<td>America/Thunder_Bay</td>
</tr>
<tr>
<td>America/Belem</td>
<td>America/Lima</td>
<td>America/Tijuana</td>
</tr>
<tr>
<td>America/Belize</td>
<td>America/Los_Angeles</td>
<td>America/Toronto</td>
</tr>
<tr>
<td>America/Blanc-Sablon</td>
<td>America/Louisville</td>
<td>America/Tortola</td>
</tr>
<tr>
<td>America/Boa_Vista</td>
<td>America/Lower_Prices</td>
<td>America/Vancouver</td>
</tr>
<tr>
<td>America/Bogota</td>
<td>America/Maceio</td>
<td>America/Virgin</td>
</tr>
<tr>
<td>America/Boise</td>
<td>America/Managua</td>
<td>America/Whitehorse</td>
</tr>
<tr>
<td>America/Buenos_Aires</td>
<td>America/Manaus</td>
<td>America/Winnipeg</td>
</tr>
<tr>
<td>America/Cambridge_Bay</td>
<td>America/Marigot</td>
<td>America/Yakutat</td>
</tr>
<tr>
<td>America/Campo_Grande</td>
<td>America/Martinique</td>
<td>America/Yellowknife</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>America/Cancun</td>
<td>America/Matamoros</td>
<td>Brazil/Acre</td>
</tr>
<tr>
<td>America/Caracas</td>
<td>America/Mazatlan</td>
<td>Brazil/DeNoronha</td>
</tr>
<tr>
<td>America/Catamarca</td>
<td>America/Mendoza</td>
<td>Brazil/East</td>
</tr>
<tr>
<td>America/Cayenne</td>
<td>America/Menominee</td>
<td>Brazil/West</td>
</tr>
<tr>
<td>America/Cayman</td>
<td>America/Merida</td>
<td>Canada/Atlantic</td>
</tr>
<tr>
<td>America/Chicago</td>
<td>America/Matlakatla</td>
<td>Canada/Central</td>
</tr>
<tr>
<td>America/Chihuahua</td>
<td>America/Mexico_City</td>
<td>Canada/East</td>
</tr>
<tr>
<td>America/Coral_Harbour</td>
<td>America/Miquelon</td>
<td>Canada/East-Saskatchewan</td>
</tr>
<tr>
<td>America/Cordoba</td>
<td>America/Moncton</td>
<td>Canada/Mountain</td>
</tr>
<tr>
<td>America/Costa_Rica</td>
<td>America/Monterrey</td>
<td>Canada/Newfoundland</td>
</tr>
<tr>
<td>America/Creston</td>
<td>America/Monterideo</td>
<td>Canada/Pacific</td>
</tr>
<tr>
<td>America/Cuiaba</td>
<td>America/Montreal</td>
<td>Canada/Saskatchewan</td>
</tr>
<tr>
<td>America/Curacao</td>
<td>America/Montserrat</td>
<td>Canada/Yukon</td>
</tr>
<tr>
<td>America/Danmarkshavn</td>
<td>America/Nassau</td>
<td>Chile/Continental</td>
</tr>
<tr>
<td>America/Dawson</td>
<td>America/New_York</td>
<td>Chile/EasterIsland</td>
</tr>
<tr>
<td>America/Dawson_Creek</td>
<td>America/Nipigon</td>
<td>Cuba</td>
</tr>
<tr>
<td>America/Denver</td>
<td>America/Nome</td>
<td>Jamaica</td>
</tr>
<tr>
<td>America/Detroit</td>
<td>America/Noronha</td>
<td>Mexico/BajaNorte</td>
</tr>
<tr>
<td>America/Dominica</td>
<td>America/North_Dakota/Beulah</td>
<td>Mexico/BajaSur</td>
</tr>
<tr>
<td>America/Edmonton</td>
<td>America/North_Dakota/Center</td>
<td>Mexico/General</td>
</tr>
<tr>
<td>America/Eirunepe</td>
<td>America/North_Dakota/New_Salem</td>
<td>US/Alaska</td>
</tr>
<tr>
<td>America/El_Salvador</td>
<td>America/Ojinaga</td>
<td>US/Aleutian</td>
</tr>
<tr>
<td>America/Ensenada</td>
<td>America/Panama</td>
<td>US/Arizona</td>
</tr>
<tr>
<td>America/Fort_Wayne</td>
<td>America/Pangnirtung</td>
<td>US/Central</td>
</tr>
<tr>
<td>America/Fortaleza</td>
<td>America/Paramaribo</td>
<td>US/East</td>
</tr>
<tr>
<td>America/Glace_Bay</td>
<td>America/Phoenix</td>
<td>US/East-Indiana</td>
</tr>
<tr>
<td>America/Godthab</td>
<td>America/Port_of_Spain</td>
<td>US/Indiana-Starke</td>
</tr>
<tr>
<td>America/Goose_Bay</td>
<td>America/Port-au-Prince</td>
<td>US/Michigan</td>
</tr>
<tr>
<td>America/Grand_Turk</td>
<td>America/Porto_Acre</td>
<td>US/Mountain</td>
</tr>
<tr>
<td>America/Grenada</td>
<td>America/Porto_Velho</td>
<td>US/Pacific</td>
</tr>
<tr>
<td>America/Guadeloupe</td>
<td>America/Puerto_Rico</td>
<td>US/Pacific-New</td>
</tr>
</tbody>
</table>
### Oceanic time zone settings

**IMPORTANT:** Time zones must be entered exactly as they appear.

The following table provides the Oceanic time zone settings that are supported by the Onboard Administrator.

<table>
<thead>
<tr>
<th>Atlantic/Azores</th>
<th>Australia/Melbourne</th>
<th>Kwajalein</th>
<th>Pacific/Marquesas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Atlantic/Bermuda</td>
<td>Australia/North</td>
<td>NZ</td>
<td>Pacific/Midway</td>
</tr>
<tr>
<td>Atlantic/Canary</td>
<td>Australia/NSW</td>
<td>NZ-CHAT</td>
<td>Pacific/Nauru</td>
</tr>
<tr>
<td>Atlantic/Cape_Verde</td>
<td>Australia/Perth</td>
<td>Pacific/Apia</td>
<td>Pacific/Niue</td>
</tr>
<tr>
<td>Atlantic/Faeroe</td>
<td>Australia/Queensland</td>
<td>Pacific/Auckland</td>
<td>Pacific/Norfolk</td>
</tr>
<tr>
<td>Atlantic/Jan_Mayen</td>
<td>Australia/South</td>
<td>Pacific/Chatham</td>
<td>Pacific/Noumea</td>
</tr>
<tr>
<td>Atlantic/Madeira</td>
<td>Australia/Sydney</td>
<td>Pacific/Chuuk</td>
<td>Pacific/Pago_Pago</td>
</tr>
<tr>
<td>Atlantic/Reykjavik</td>
<td>Australia/Tasmania</td>
<td>Pacific/Easter</td>
<td>Pacific/Palau</td>
</tr>
<tr>
<td>Atlantic/South_Georgia</td>
<td>Australia/Victoria</td>
<td>Pacific/Elate</td>
<td>Pacific/Pitcairn</td>
</tr>
<tr>
<td>Atlantic/St_Helena</td>
<td>Australia/West</td>
<td>Pacific/Enderbury</td>
<td>Pacific/Pohnpei</td>
</tr>
<tr>
<td>Atlantic/Stanley</td>
<td>Australia/Yancowinna</td>
<td>Pacific/Fakaofo</td>
<td>Pacific/Ponape</td>
</tr>
<tr>
<td>Australia/ACT</td>
<td>Iceland</td>
<td>Pacific/Fiji</td>
<td>Pacific/Port_Moresby</td>
</tr>
<tr>
<td>Australia/Adelaide</td>
<td>Indian/Antananarivo</td>
<td>Pacific/Funafuti</td>
<td>Pacific/Rarotonga</td>
</tr>
<tr>
<td>Australia/Brisbane</td>
<td>Indian/Chagos</td>
<td>Pacific/Galapagos</td>
<td>Pacific/Saipan</td>
</tr>
<tr>
<td>Australia/Broken_Hill</td>
<td>Indian/Christmas</td>
<td>Pacific/Gambier</td>
<td>Pacific/Samoa</td>
</tr>
<tr>
<td>Australia/Canberra</td>
<td>Indian/Cocos</td>
<td>Pacific/Guadalcanal</td>
<td>Pacific/Tahiti</td>
</tr>
<tr>
<td>Australia/Currie</td>
<td>Indian/Comoro</td>
<td>Pacific/Guam</td>
<td>Pacific/Tarawa</td>
</tr>
</tbody>
</table>
## Europe time zone settings

**IMPORTANT:** Time zones must be entered exactly as they appear.

The following table provides the European time zone settings that are supported by the Onboard Administrator.

<table>
<thead>
<tr>
<th>Country</th>
<th>Time Zone</th>
<th>Time Zone</th>
<th>Time Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eire</td>
<td>Europe/Kaliningrad</td>
<td>Europe/Sarajevo</td>
<td></td>
</tr>
<tr>
<td>Europe/Amsterdam</td>
<td>Europe/Kiev</td>
<td>Europe/Sarajevo</td>
<td></td>
</tr>
<tr>
<td>Europe/Andorra</td>
<td>Europe/Lisbon</td>
<td>Europe/Sarajevo</td>
<td></td>
</tr>
<tr>
<td>Europe/Athens</td>
<td>Europe/Ljubljana</td>
<td>Europe/Sofia</td>
<td></td>
</tr>
<tr>
<td>Europe/Belfast</td>
<td>Europe/London</td>
<td>Europe/Stockholm</td>
<td></td>
</tr>
<tr>
<td>Europe/Belgrade</td>
<td>Europe/Luxembourg</td>
<td>Europe/Tallinn</td>
<td></td>
</tr>
<tr>
<td>Europe/Berlin</td>
<td>Europe/Madrid</td>
<td>Europe/Tirane</td>
<td></td>
</tr>
<tr>
<td>Europe/Bratislava</td>
<td>Europe/Malta</td>
<td>Europe/Tiraspol</td>
<td></td>
</tr>
<tr>
<td>Europe/Brussels</td>
<td>Europe/Monchengen</td>
<td>Europe/Uzhgorod</td>
<td></td>
</tr>
<tr>
<td>Europe/Bucharest</td>
<td>Europe/Minsk</td>
<td>Europe/Vaduz</td>
<td></td>
</tr>
<tr>
<td>Europe/Budapest</td>
<td>Europe/Monaco</td>
<td>Europe/Vatican</td>
<td></td>
</tr>
<tr>
<td>Europe/Busingen</td>
<td>Europe/Moscow</td>
<td>Europe/Vienna</td>
<td></td>
</tr>
<tr>
<td>Europe/Chisinau</td>
<td>Europe/Nicosia</td>
<td>Europe/Vilnius</td>
<td></td>
</tr>
<tr>
<td>Europe/Copenhagen</td>
<td>Europe/Oslo</td>
<td>Europe/Volgograd</td>
<td></td>
</tr>
<tr>
<td>Europe/Dublin</td>
<td>Europe/Paris</td>
<td>Europe/Warsaw</td>
<td></td>
</tr>
<tr>
<td>Europe/Gibraltar</td>
<td>Europe/Portgorica</td>
<td>Europe/Zagreb</td>
<td></td>
</tr>
<tr>
<td>Europe/Guernsey</td>
<td>Europe/Prague</td>
<td>Europe/Zaporozhye</td>
<td></td>
</tr>
<tr>
<td>Europe/Helsinki</td>
<td>Europe/Riga</td>
<td>Europe/Zurich</td>
<td></td>
</tr>
<tr>
<td>Europe/Isle_of_Man</td>
<td>Europe/Rome</td>
<td>GB</td>
<td></td>
</tr>
<tr>
<td>Europe/Istanbul</td>
<td>Europe/Samara</td>
<td>GB/Eire</td>
<td></td>
</tr>
<tr>
<td>Europe/Jersey</td>
<td>Europe/San Marino</td>
<td>Poland</td>
<td></td>
</tr>
<tr>
<td>—</td>
<td>—</td>
<td>—</td>
<td>GB</td>
</tr>
</tbody>
</table>

## Polar time zone settings

**IMPORTANT:** Time zones must be entered exactly as they appear.

The following table provides the Polar time zone settings that are supported by the Onboard Administrator.

<table>
<thead>
<tr>
<th>Zone</th>
<th>Time Zone</th>
<th>Time Zone</th>
<th>Time Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antarctica/Casey</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Antarctica/Mawson</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Antarctica/South_Pole</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>---------------</td>
<td>---------------</td>
<td></td>
</tr>
<tr>
<td>Antarctica/Davis</td>
<td>Antarctica/McMurdo</td>
<td>Antarctica/Syowa</td>
<td></td>
</tr>
<tr>
<td>Antarctica/DumontDUrville</td>
<td>Antarctica/Palmer</td>
<td>Antarctica/Vostok</td>
<td></td>
</tr>
<tr>
<td>Antarctica/Macquarie</td>
<td>Antarctica/Rothera</td>
<td>Arctic/Longyearbyen</td>
<td></td>
</tr>
</tbody>
</table>
Acronyms and abbreviations

BLD
BladeSystem Location Device

CA
certificate authority

DDNS
Dynamic Domain Name System

DHCP
Dynamic Host Configuration Protocol

DN
distinguished name

DNS
domain name system

EBIPA
Enclosure Bay IP Addressing

EFM
Enclosure Firmware Management

ext2
second extended file system

FAT32
File Allocation Table with cluster values represented by 32-bit numbers

FQDN
Fully Qualified Domain Name

FRU
field replaceable unit
GC
global catalog

HDD
hard disk drive or hard drive

HP SIM
HP Systems Insight Manager

HTTPS
hypertext transfer protocol secure sockets

ICMP
Internet Control Message Protocol

iLO
Integrated Lights-Out

IPD
intelligent power discovery

IPMI
Intelligent Platform Management Interface

JSON
JavaScript Object Notation

LDAP
Lightweight Directory Access Protocol

MAC
Media Access Control

NTP
network time protocol

PDU
power distribution unit

PIC
peripheral interface controller
PKCS
Public-Key Cryptography Standards

PXE
preboot execution environment

RBSU
ROM-Based Setup Utility

RIBCL
Remote Insight Board Command Language

RSA
Rivest, Shamir, and Adelman public encryption key

SLAAC
stateless address autoconfiguration

SOAP
Simple Object Access Protocol

SSH
Secure Shell

SSO
single sign-on

TFTP
Trivial File Transfer Protocol

TPM
Trusted Platform Module

UEFI
Unified Extensible Firmware Interface

UID
unit identification

URB
utility ready blade
VC
Virtual Connect

VCM
Virtual Connect Manager

WWN
World Wide Name
HP is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (mailto:docsfeedback@hp.com). Include the document title and part number, version number, or the URL when submitting your feedback.
A
accessing the CLI 14
account authentication 19
account level 17
ADD CA CERTIFICATE 35
ADD EBIPA 61
ADD EBIPAV6 61
ADD HPSIM CERTIFICATE 49
ADD LANGUAGE 122
ADD LDAP CERTIFICATE 40
ADD LDAP GROUP 40
ADD OA ADDRESS IPV6 77
ADD OA DNS 77
ADD OA DNS IPV6 78
ADD OA ROUTE IPV6 79
ADD REMOTE_SUPPORT CERTIFICATE 213
ADD SNMP TRAPRECEIVER 80, 81
ADD SNMP USER 82
ADD SSHKEY 79
ADD TRUSTED HOST 83
ADD VLAN 207
Africa time zone 228
Americas time zone 229
Asia time zone 230
ASSIGN 26
ASSIGN FOR LDAP 41
ASSIGN INTERCONNECT 187
ASSIGN OA 27
ASSIGN OA LDAP GROUP 41
ASSIGN SERVER 168
authorized reseller 226

B
Blade management commands 168
boot mode 175

C
ciphers 90, 98
CLEAR FIRMWARE MANAGEMENT ALL_LOGS 157
CLEAR INTERCONNECT SESSION 187
CLEAR LOGIN_BANNER_TEXT 84
CLEAR NTP 84
CLEAR SCREEN 21
CLEAR SSHKEY 84
CLEAR SYSLOG 122
CLEAR VCMODE 84
CLI (Command Line Interface) 16
command line, Event messages 223
command, 188, 210
command, ADD CA CERTIFICATE 35
command, ADD EBIPA 61
command, ADD EBIPAV6 61
command, ADD HPSIM CERTIFICATE 49
command, ADD LANGUAGE 122
command, ADD LDAP CERTIFICATE 40
command, ADD LDAP GROUP 40
command, ADD OA ADDRESS IPV6 77
command, ADD OA DNS 77
command, ADD OA DNS IPV6 78
command, ADD OA ROUTE IPV6 79
command, ADD REMOTE_SUPPORT CERTIFICATE 213
command, ADD SNMP TRAPRECEIVER 80, 81
command, ADD SNMP USER 82
command, ADD SSHKEY 79
command, ADD TRUSTED HOST 83
command, ADD VLAN 207
command, ASSIGN 26
command, ASSIGN for LDAP 41
command, ASSIGN INTERCONNECT 187
command, ASSIGN OA 27
command, ASSIGN OA LDAP GROUP 41
command, ASSIGN SERVER 168
command, CLEAR FIRMWARE MANAGEMENT ALL_LOGS 157
command, CLEAR INTERCONNECT SESSION 187
command, CLEAR LOGIN_BANNER_TEXT 84
command, CLEAR NTP 84
command, CLEAR SCREEN 21
command, CLEAR SSHKEY 84
command, CLEAR SYSLOG 122
command, CLEAR VCMODE 84
command, CONNECT ENCLOSURE 122
command, CONNECT INTERCONNECT 187
command, CONNECT SERVER 168
command, DISABLE ACTIVE HEALTH SYSTEM 198

Index  239
command, DISABLE ALERTMAIL  85
command, DISABLE CRL   35
command, DISABLE DHCP_DOMAIN_NAME  123
command, DISABLE DHCPV6  85
command, DISABLE EBIPA  61
command, DISABLE EBIPAV6  62
command, DISABLE ENCLOSURE_ILO_FEDERATION_SUPPORT  85
command, DISABLE ENCLOSURE_IP_MODE  86
command, DISABLE FIRMWARE MANAGEMENT  157
command, DISABLE FQDN_LINK_SUPPORT  86
command, DISABLE GUI_LOGIN_DETAIL  123
command, DISABLE HTTPS  86
command, DISABLE IPV6  87
command, DISABLE IPV6DYNDNS  87
command, DISABLE LDAP  41
command, DISABLE LLF  123
command, DISABLE LOGIN_BANNER  88
command, DISABLE NTP  88
command, DISABLE REMOTE SUPPORT  216
command, DISABLE REMOTE SUPPORT MAINTENANCE  216
command, DISABLE SECURESH  89
command, DISABLE SLAAC  89
command, DISABLE SNMP  89
command, DISABLE SSL_CIPHER  90
command, DISABLE STRONG_PASSWORDS  27
command, DISABLE SYSLOG_REMOTE  201
command, DISABLE TELNET  91
command, DISABLE TRUSTED_HOST  91
command, DISABLE TWOFACTOR  36
command, DISABLE URB  52
command, DISABLE USER  27
command, DISABLE VLAN  207
command, DISABLE XMLREPLY  91
command, DISCOVER_FIRMWARE_SERVER  157
command, DOWNLOAD CA_CERTIFICATE  36
command, DOWNLOAD_CONFIG  92
command, DOWNLOAD_CONFIG using USB key  204
command, DOWNLOAD_HPSIM_CERTIFICATE  49
command, DOWNLOAD_LDAP_CERTIFICATE  42
command, DOWNLOAD_OA_CERTIFICATE  52
command, DOWNLOAD_REMOTE_SUPPORT_CERTIFICATE  213
command, DOWNLOAD_SSHKEY  92
command, DOWNLOAD_USER_CERTIFICATE  36
command, EDIT_VLAN  207
command, ENABLE ACTIVE_HEALTH_SYSTEM  198
command, ENABLE ALERTMAIL  93
command, ENABLE DHCP_DOMAIN_NAME  124
command, ENABLE DHCPV6  93
command, ENABLE EBIPA  62
command, ENABLE EBIPAV6  63
command, ENABLE ENCLOSURE_ILO_FEDERATION_SUPPORT  93
command, ENABLE ENCLOSURE_IP_MODE  94
command, ENABLE FIRMWARE MANAGEMENT  158
command, ENABLE FQDN_LINK_SUPPORT  94
command, ENABLE GUI_LOGIN_DETAIL  124
command, ENABLE HTTPS  95
command, ENABLE IPV6  95
command, ENABLE IPV6DYNDNS  95
command, ENABLE LDAP  42
command, ENABLE LLF  124
command, ENABLE LOGIN_BANNER  96
command, ENABLE NTP  96
command, ENABLE REMOTE_SUPPORT IRS  215
command, ENABLE REMOTE_SUPPORT MAINTENANCE  215
command, ENABLE REMOTE_SUPPORT DIRECT  214
command, ENABLE ROUTER_ADVERTISEMENTS  96
command, ENABLE SECURESH  97
command, ENABLE SLAAC  97
command, ENABLE SNMP  97
command, ENABLE SSL_CIPHER  98
command, ENABLE SSL_PROTOCOL  98
command, ENABLE STRONG_PASSWORDS  28
command, ENABLE SYSLOG_REMOTE  201
command, ENABLE TELNET  99
command, ENABLE TRUSTED_HOST  99
command, ENABLE URB  53
command, ENABLE USER  28
command, ENABLE VLAN  208
command, ENABLE XMLREPLY  99
command, EXIT  21
command, FORCE TAKEOVER  53
command, GENERATE_CERTIFICATE  53
command, GENERATE_KEY  55
command, HELP  21
command, HISTORY  28
command, HPONCFG  168
command, LOGOUT  21
command, PING  56
command, POWEROFF_INTERCONNECT  188
command, POWEROFF_SERVER  170
command, POWERON_INTERCONNECT  188
command, POWERON_SERVER  170
command, QUIT  22
command, REBOOT_SERVER  171
command, REMOVE CA CERTIFICATE  37
command, REMOVE EBIPA   63
command, REMOVE EBIPAv6  64
command, REMOVE HPSIM CERTIFICATE  50
command, REMOVE LDAP CERTIFICATE  42
command, REMOVE LDAP GROUP  43
command, REMOVE OA ADDRESS IPV6  99
command, REMOVE OA DNS  100
command, REMOVE OA DNS IPV6  100
command, REMOVE OA ROUTE IPV6  101
command, REMOVE REMOTE_SUPPORT CERTIFICATE  216
command, REMOVE SNMP TRAPRECEIVER  101, 102
command, REMOVE SNMP USER  102
command, REMOVE TRUSTED HOST  102
command, REMOVE USER  29
command, REMOVE USER CERTIFICATE  37
command, REMOVE VLAN  208
command, RESET ILO  125
command, RESTART OA  126
command, SAVE EBIPA  64
command, SAVE EBIPAv6  65
command, SAVE VLAN  208
command, SEND REMOTE SUPPORT DATACOLLECTION  216
command, SET ALERTMAIL MAILBOX  103
command, SET ALERTMAIL SENDERDOMAIN  103
command, SET ALERTMAIL SENDERNAME  104
command, SET ALERTMAIL SMTP SERVER  104
command, SET DATE  126
command, SET
  DEVICE_SERIAL_NUMBER_BLADE  56
command, SET DISPLAY EVENTS  127
command, SET EBIPA INTERCONNECT  65
command, SET EBIPA SERVER  66
command, SET EBIPAv6 INTERCONNECT  67
command, SET EBIPAv6 SERVER  68
command, SET ENCLOSURE ASSET  129
command, SET ENCLOSURE NAME  130
command, SET ENCLOSURE PART_NUMBER  130
command, SET ENCLOSURE PDU TYPE  130
command, SET ENCLOSURE POWER_CAP  221
command, SET ENCLOSURE
  POWER_CAP_BAYS_TO_EXCLUDE  221
command, SET ENCLOSURE SERIAL_NUMBER  131
command, SET ENCLOSURE UID  131
command, SET FACTORY  57
command, SET FIPS MODE  104
command, SET FIRMWARE MANAGEMENT  158
command, SET FIRMWARE MANAGEMENT BAYS_TO_INCLUDE SERVER  160
command, SET FIRMWARE MANAGEMENT FORCE DOWNGRADE  160
command, SET FIRMWARE MANAGEMENT POLICY  159
command, SET FIRMWARE MANAGEMENT POWER  159
command, SET FIRMWARE MANAGEMENT SCHEDULE  160
command, SET FIRMWARE MANAGEMENT URL  158
command, SET HPSIM TRUST MODE  50
command, SET HTTP REQUESTREADTIMEOUT  105
command, SET INTERCONNECT
  ADMIN_PASSWORD FACTORY  189
command, SET INTERCONNECT
  POWERDELAY  190
command, SET INTERCONNECT UID  190
command, SET IPCONFIG  106
command, SET LDAP GCPORT  44
command, SET LDAP GROUP ACCESS  43
command, SET LDAP GROUP DESCRIPTION  43
command, SET LDAP NAME  44
command, SET LDAP PORT  44
command, SET LDAP SERVER  45
command, SET LLF INTERVAL  131
command, SET LOGIN_BANNER_TEXT  107
command, SET MINIMUM PASSWORD LENGTH  29
command, SET NIC  171
command, SET NTP POLL  107
command, SET NTP PRIMARY  108
command, SET NTP SECONDARY  108
command, SET OA DOMAIN_NAME  132
command, SET OA GATEWAY  108
command, SET OA GATEWAY IPV6  109
command, SET OA NAME  109
command, SET OA UID  109
command, SET OA USB  132
command, SET PASSWORD  29
command, SET POWER LIMIT  133
command, SET POWER MODE  133
command, SET POWER SAVINGS  134
command, SET RACK NAME  23
command, SET REMOTE SYSLOG PORT  201
command, SET REMOTE SYSLOG SERVER  202
command, SET REMOTE_SUPPORT DIRECT
  ONLINE_REGISTRATION_COMPLETE  217
command, SET REMOTE_SUPPORT DIRECT
  PROXY  217
command, SET SCRIPT MODE  57
command, SET SECURESH SERVER KEX DHG1 110
command, SET SERIAL BAUD 110
command, SET SERVER BOOT 172
command, SET SERVER BOOT FIRST 172
command, SET SERVER DVD for USB key 204
command, SET SERVER POWERDELAY 174
command, SET SERVER UID 174
command, SET SESSION TIMEOUT 30
command, SET SNMP COMMUNITY 110
command, SET SNMP CONTACT 111
command, SET SNMP ENGINEID 111
command, SET SNMP LOCATION 112
command, SET TIME ZONE 134
command, SET URB 58
command, SET USER ACCESS 30
command, SET USER CERTIFICATE 37
command, SET USER CONTACT 30
command, SET USER FULLNAME 31
command, SET USER PASSWORD 31
command, SET VLAN DEFAULT 208
command, SET VLAN FACTORY 209
command, SET VLAN INTERCONNECT 209
command, SET VLAN IPCONFIG SAVE 210
command, SET VLAN IPCONFIG STATIC 210
command, SET VLAN OA 211
command, SET VLAN REVERT 211
command, SET VLAN SERVER 211
command, SHOW ALL 58
command, SHOW CA CERTIFICATE 38
command, SHOW CONFIG 134
command, SHOW DATE 135
command, SHOW DEVICE SERIAL NUMBER BLADE 59
command, SHOW DISPLAY EVENTS 136
command, SHOW EBIPA 70
command, SHOW EBIPAV6 73
command, SHOW ENCLOSURE FAN 136
command, SHOW ENCLOSURE INFO 136
command, SHOW ENCLOSURE LCD 137
command, SHOW ENCLOSURE POWER_CAP 222
command, SHOW ENCLOSURE POWER_CAP_BAYS_TO_EXCLUDE 222
command, SHOW ENCLOSURE POWER_SUMMARY 138
command, SHOW ENCLOSURE POWERSUPPLY 139
command, SHOW ENCLOSURE STATUS 140, 141
command, SHOW ENCLOSURE TEMP 141
command, SHOW FINGERPRINT 118
command, SHOW FIPS MODE 112
command, SHOW FIRMWARE 161
command, SHOW FIRMWARE LOG SERVER 165
command, SHOW FIRMWARE LOG SESSION 165
command, SHOW FIRMWARE MANAGEMENT 161
command, SHOW FIRMWARE MANAGEMENT LOG 162
command, SHOW FIRMWARE SUMMARY 162
command, SHOW FIRMWARE SUMMARY CSV 164
command, SHOW FRU 141
command, SHOW HEALTH 112
command, SHOW HPSIM INFO 50
command, SHOW INTERCONNECT 190
command, SHOW INTERCONNECT INFO 192
command, SHOW INTERCONNECT LIST 194
command, SHOW INTERCONNECT PORT MAP 195
command, SHOW INTERCONNECT POWERDELAY 195
command, SHOW INTERCONNECT SESSION 196
command, SHOW INTERCONNECT STATUS 196
command, SHOW LANGUAGES 144
command, SHOW LDAP CERTIFICATE 45
command, SHOW LDAP GROUP 46
command, SHOW LDAP INFO 46
command, SHOW LOGIN_BANNER 114
command, SHOW NETWORK 115
command, SHOW OA 144
command, SHOW OA CERTIFICATE 144
command, SHOW OA INFO 145
command, SHOW OA NETWORK 146
command, SHOW OA STATUS 147
command, SHOW OA UPTIME 148
command, SHOW OA USB 148
command, SHOW PASSWORD SETTINGS 32
command, SHOW RACK INFO 23
command, SHOW RACK NAME 24
command, SHOW REMOTE SUPPORT 218
command, SHOW REMOTE SUPPORT EVENTS 219
command, SHOW REMOTE_SUPPORT CERTIFICATE 218
command, SHOW SERVER BOOT 174
command, SHOW SERVER DVD 199
command, SHOW SERVER FIRMWARE 166
command, SHOW SERVER INFO 175
command, SHOW SERVER LIST 177
command, SHOW SERVER NAMES 178
command, SHOW SERVER PORT MAP 179
command, SHOW SERVER POWERDELAY 180
command, SHOW SERVER STATUS 181
command, SHOW SERVER TEMP 183
command, SHOW SESSION TIMEOUT 32
command, SHOW SNMP 117
command, SHOW SNMP USER 118
command, SHOW SSHKEY 119
command, SHOW SSL 119
command, SHOW SSL PROTOCOL 120
command, SHOW SYSLOG 149
command, SHOW SYSLOG HISTORY 151
command, SHOW SYSLOG OA 150
command, SHOW SYSLOG SERVER 184
command, SHOW SYSLOG SETTINGS 202
command, SHOW TOPOLOGY 24
command, SHOW TWOFACTOR INFO 39
command, SHOW URB 59
command, SHOW USBKEY 204
command, SHOW USER 33
command, SHOW VCMODE 120
command, SHOW VLAN 211
cmand, SLEEP 33
command, TEST ALERTMAIL 120
command, TEST LDAP 47
command, TEST REMOTE_SUPPORT 219
command, TEST SNMP 121
command, TEST SYSLOG 202
command, TEST URB 59
command, UNASSIGN 33
command, UNASSIGN FOR LDAP 47
command, UNASSIGN OA 34
command, UNASSIGN OA LDAP GROUP 47
command, UNASSIGN SERVER 185
command, UPDATE 152
command, UPDATE FIRMWARE SERVER 166
command, UPDATE ILO 153
command, UPDATE IMAGE 153
command, UPDATE IMAGE using USB key 205
command, UPLOAD CONFIG 154
command, UPLOAD CONFIG using USB key 206
command, UPLOAD SUPPORTDUMP 155
command, UPLOAD SYSLOG 155
commands, directory 40
commands, remote support 213
CONNECT ENCLOSURE 122
CONNECT INTERCONNECT 187
CONNECT SERVER 168
Current Default Gateway 108, 109, 115, 146

D
default gateway 108, 115, 146
DHCP addresses 93, 106
directory (LDAP) commands 40
DISABLE ACTIVE HEALTH SYSTEM 198
DISABLE ALERTMAIL 85
DISABLE CRL 35
DISABLE DHCP_DOMAIN_NAME 123
DISABLE DHCPv6 85
DISABLE EBIPA 61
DISABLE EBIPAV6 62
DISABLE ENCLOSURE_ILO_FEDERATION_SUPPORT 85
DISABLE ENCLOSURE_IP_MODE 86
DISABLE FIRMWARE MANAGEMENT 157
DISABLE FQDN_LINK_SUPPORT 86
DISABLE GUI_LOGIN_DETAIL 123
DISABLE HTTPS 86
DISABLE IPV6 87
DISABLE IPV6DYNDNS 87
DISABLE LDAP 41
DISABLE LLF 123
DISABLE LOGIN_BANNER 88
DISABLE NTP 88
DISABLE REMOTE SUPPORT 216
DISABLE REMOTE SUPPORT MAINTENANCE 216
DISABLE SECURESH 89
DISABLE SLAAC 89
DISABLE SNMP 89
DISABLE SSL CIPHER 90
DISABLE SSL PROTOCOL 90
DISABLE STRONG PASSWORDS 27
DISABLE SYSLOGREMOTE 201
disable telnet 91
DISABLE TRUSTED HOST 91
DISABLE TWOFACTOR 36
DISABLE URB 52
DISABLE USER 27
DISABLE VLAN 207
DISABLE XMLREPLY 91
DISCOVER FIRMWARE SERVER 157
DNS server 77, 78, 100
documentation 227, 238
documentation feedback 238
DOWNLOAD CA CERTIFICATE 36
DOWNLOAD CONFIG 92
DOWNLOAD CONFIG using USB key 204
DOWNLOAD HPSIM CERTIFICATE 49
DOWNLOAD LDAP CERTIFICATE 42
DOWNLOAD OA CERTIFICATE 52
DOWNLOAD REMOTE_SUPPORT CERTIFICATE 213
DOWNLOAD SSHKEY 92
DOWNLOAD USER CERTIFICATE 36
dynamic DNS 95, 106
EDIT VLAN 207
ENABLE ACTIVE HEALTH SYSTEM 198
ENABLE ALERTMAIL 93
ENABLE DHCPV6 93
ENABLE DISABLE DHCP_DOMAIN_NAME 124
ENABLE EBIPA 62
ENABLE EBIPAV6 63
ENABLE ENCLOSURE_ILO_FEDERATION_SUPPORT 93
ENABLE ENCLOSURE_IP_MODE 94
ENABLE FIRMWARE MANAGEMENT 158
ENABLE FQDN_LINK_SUPPORT 94
ENABLE GUI_LOGIN_DETAIL 124
ENABLE HTTPS 95
ENABLE IPV6 95
ENABLE IPV6DYNDNS 95
ENABLE LDAP 42
ENABLE LLF 124
ENABLE LOGIN_BANNER 96
ENABLE NTP 96
ENABLE REMOTE_SUPPORT IRS 215
ENABLE REMOTE_SUPPORT MAINTENANCE 215
ENABLE REMOTE_SUPPORT DIRECT 214
ENABLE ROUTER_ADVERTISEMENTS 96
ENABLE SECURESH 97
ENABLE SLAAC 97
ENABLE SNMP 97
ENABLE SSL_CIPHER 98
ENABLE SSL_PROTOCOL 98
ENABLE STRONG_PASSWORDS 28
ENABLE SYSLOG_REMOTE 201
ENABLE TELNET 99
ENABLE TRUSTED_HOST 99
ENABLE URB 53
ENABLE USER 28
ENABLE VLAN 208
ENABLE XMLPREPLY 99
Enclosure Bay IP Addressing (EBIPA) commands 61
capture DVD commands 199
Enclosure Firmware Management commands 157
capture enclosure management commands 122
Enclosure network configuration commands 77
Europe time zone 232
event notifications, defining 223
EXIT 21
extended system log 151

FIPS Mode, enabling 104
firmware management log 157
force downgrades 153
FORCE TAKEOVER 53
FQDN link support 94
gateway, static route 79, 101, 115, 146
general commands 21
general management commands 52
Generate certificate prompts 54
GENERATE_CERTIFICATE 53
GENERATE_KEY 55
HELP 21
help resources 226
HISTORY 28
HP SIM commands 49
HPONCFG 168
HTTP Request Read Timeout 105, 115
iLO AutoLogin 19
Integrity blade restrictions 17
Interconnect management commands 187
Linux support 16
local access 14
LOGOUT 21
network settings 115, 146
Oceanic time zone 231
PING 56
polar time zone 232
POWEROFF_INTERCONNECT 188
POWEROFF_SERVER 170
POWERON_INTERCONNECT 188
POWERON_SERVER 170
privilege levels 17, 19

Q
QUIT 22

R
rack commands 23
rack settings 23
REBOOT SERVER 171
remote access 14
Remote support commands 213
remote syslog commands 201
remote system logging 203
REMOVE CA CERTIFICATE 37
REMOVE EBIPA 63
REMOVE EBIPAv6 64
REMOVE HPSIM CERTIFICATE 50
REMOVE LDAP CERTIFICATE 42
REMOVE LDAP GROUP 43
REMOVE OA ADDRESS IPV6 99
REMOVE OA DNS 100
REMOVE OA DNS IPV6 100
REMOVE OA ROUTE IPV6 101
REMOVE REMOTE_SUPPORT CERTIFICATE 216
REMOVE SNMP TRAPRECEIVER 101, 102
REMOVE SNMP USER 102
REMOVE TRUSTED HOST 102
REMOVE USER 29
REMOVE USER CERTIFICATE 37
REMOVE VLAN 208
reserved words 16
RESET ILO 125
RESTART INTERCONNECT 188
RESTART OA 126
restrictions, Integrity blade 17
router advertisements 88, 96, 115, 146

S
SAVE EBIPA 64
SAVE EBIPAv6 65
SAVE VLAN 208
Secure Boot 175
security ciphers 90, 98
security protocols 90, 98
security settings 90, 91, 98
SEND REMOTE SUPPORT DATACOLLECTION 216
serial port 14
SET ALERTMAIL MAILBOX 103
SET ALERTMAIL SENDERDOMAIN 103

set alertmail sendernamE 104
set alertmail sm 104
set date 126
set device serial_number blade 56
set display 127
set ebipa interconnect 65
set ebipAv6 interconnect 67
set ebipAv6 server 68
set enclosure asset 129
set enclosure name 130
set enclosure part number 130
set enclosure pdu type 130
set enclosure power_cap 221
set enclosure power_cap_bays_to_exclude 221
set enclosure serial_number 131
set enclosure uid 131
set factory 57
set fips mode 104
set firmware management 158
set firmware management bays_to_include server 160
set firmware management force downgrade 160
set firmware management policy 159
set firmware management power 159
set firmware management schedule 160
set firmware management url 158
set hpsim trust mode 50
set http requestreadtimeout 105
set interconnect admin_password factory 189
set interconnect factory 189
set interconnect powerdelay 190
set interconnect uid 190
set ipconfig 106
set ldap gcport 44
set ldap group access 43
set ldap group description 43
set ldap name map 44
set ldap port 44
set ldap server 45
set llf interval 131
set login_banner_text 107
set minimum password length 29
set nic 171
set ntp poll 107
set ntp primary 108
set ntp secondary 108
set oa domain_name 132
SET OA GATEWAY 108
SET OA GATEWAY IPV6 109
SET OA NAME 109
SET OA UID 109
SET OA USB 132
SET PASSWORD 29
SET POWER LIMIT 133
SET POWER MODE 133
SET POWER SAVINGS 134
SET RACK NAME 23
SET REMOTE SYSLOG PORT 201
SET REMOTE SYSLOG SERVER 202
SET REMOTE_SUPPORT DIRECT
ONLINE_REGISTRATION_COMPLETE 217
SET REMOTE_SUPPORT DIRECT PROXY 217
SET SCRIPT MODE 57
SET SECURESH SERVER KEX DHG1 110
SET SERIAL BAUD 110
SET SERVER BOOT 172
SET SERVER BOOT FIRST 172
SET SERVER BOOT ONCE 173
SET SERVER DVD for USB key 204
SET SERVER POWERDELAY 174
SET SERVER UID 174
SET SESSION TIMEOUT 30
SET SNMP COMMUNITY 110
SET SNMP CONTACT 111
SET SNMP ENGINEID 111
SET SNMP LOCATION 112
SET TIME ZONE 134
SET URB 58
SET USER ACCESS 30
SET USER CERTIFICATE 37
SET USER CONTACT 30
SET USER FULLNAME 31
SET USER PASSWORD 31
SET VLAN DEFAULT 208
SET VLAN FACTORY 209
SET VLAN INTERCONNECT 209
SET VLAN IPCONFIG DHCP 210
SET VLAN IPCONFIG SAVE 210
SET VLAN IPCONFIG STATIC 210
SET VLAN OA 211
SET VLAN REVERT 211
SET VLAN SERVER 211
SHOW ALL 58
SHOW CA CERTIFICATE 38
SHOW CONFIG 134
SHOW DATE 135
SHOW DEVICE SERIAL_NUMBER BLADE 59
SHOW DISPLAY EVENTS 136
SHOW EBIPA 70
SHOW EBIPAV6 73
SHOW ENCLOSURE FAN 136
SHOW ENCLOSURE INFO 136
SHOW ENCLOSURE LCD 137
SHOW ENCLOSURE POWER_CAP 222
SHOW ENCLOSURE POWER_CAP_BAYS_TO_EXCLUDE 222
SHOW ENCLOSURE POWER_SUMMARY 138
SHOW ENCLOSURE POWERSUPPLY 139
SHOW ENCLOSURE STATUS 140
SHOW ENCLOSURE TEMP 141
SHOW FIPS MODE 112
SHOW FIRMWARE 161
SHOW FIRMWARE LOG SERVER 165
SHOW FIRMWARE LOG SESSION 165
SHOW FIRMWARE MANAGEMENT 161
SHOW FIRMWARE MANAGEMENT LOG 162
SHOW FIRMWARE SUMMARY 162
SHOW FIRMWARE SUMMARY CSV 164
SHOW FRU 141
SHOW HEALTH 112
SHOW HPSIM INFO 50
SHOW INTERCONNECT 190
SHOW INTERCONNECT INFO 192
SHOW INTERCONNECT LIST 194
SHOW INTERCONNECT PORT MAP 195
SHOW INTERCONNECT POWERDELAY 195
SHOW INTERCONNECT SESSION 196
SHOW INTERCONNECT STATUS 196
SHOW LANGUAGES 144
SHOW LDAP CERTIFICATE 45
SHOW LDAP GROUP 46
SHOW LDAP INFO 46
SHOW LOGIN_BANNER 114
SHOW NETWORK 115
SHOW OA 144
SHOW OA CERTIFICATE 144
SHOW OA INFO 145
SHOW OA NETWORK 146
SHOW OA STATUS 147
SHOW OA UPTIME 148
SHOW OA USB 148
SHOW PASSWORD SETTINGS 32
SHOW RACK INFO 23
SHOW RACK NAME 24
SHOW REMOTE SUPPORT 218
SHOW REMOTE SUPPORT EVENTS 219
SHOW REMOTE_SUPPORT CERTIFICATE 218
SHOW SERVER BOOT 174
SHOW SERVER DVD 199
SHOW SERVER FIRMWARE 166
SHOW SERVER INFO 175
SHOW SERVER LIST 177
SHOW SERVER NAMES 178
SHOW SERVER PORT MAP 179
SHOW SERVER POWERDELAY 180
SHOW SERVER STATUS 181
SHOW SERVER TEMP 183
SHOW SESSION TIMEOUT 32
SHOW SNMP 117
SHOW SNMP USER 118
SHOW SSHFINGERPRINT 118
SHOW SSHKEY 119
SHOW SSL CIPHER 119
SHOW SSL PROTOCOL 120
SHOW SYSLOG 149
SHOW SYSLOG HISTORY 151
SHOW SYSLOG OA 150
SHOW SYSLOG SERVER 184
SHOW SYSLOG SETTINGS 202
SHOW TOPOLOGY 24
SHOW TWOFACTOR INFO 39
SHOW URB 59
SHOW USBKEY 204
SHOW USER 33
SHOW VCMODE 120
SHOW VLAN 211
SLEEP 33
SSH session 14
Static Default 109, 115, 146
static route 79, 101, 115, 146
system log, extended 151

T

technical support 226
telnet session 14
terminal emulator session 14
TEST ALERTMAIL 120
TEST LDAP 47
TEST REMOTE_SUPPORT 219
TEST SNMP 121
TEST SYSLOG 202
TEST URB 59
Two-Factor Authentication commands 35

U

UNASSIGN 33
UNASSIGN FOR LDAP 47
UNASSIGN OA 34

UNASSIGN OA LDAP GROUP 47
UNASSIGN SERVER 185
universal time zone 228
UPDATE 152
UPDATE Firmware SERVER 166
UPDATE ILO 153
UPDATE IMAGE 153
UPDATE IMAGE using USB key 205
UPLOAD CONFIG 154
UPLOAD CONFIG using USB key 206
UPLOAD SUPPORTDUMP 155
UPLOAD SYSLOG 155
USB key command 204, 206
User account commands 26

V

VLAN commands 207

W

what's new 13