Oracle® Integrated Lights Out Manager (ILOM) 3.0

CLI Procedures Guide

Part No. 820-6412-12
October 2010, Revision A

Please
Recycle

Adobe PostScript™

Contents

Using This Documentation

This command-line interface (CLI) procedures guide describes the Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI features that are common to Oracle's Sun rack-mounted servers or server modules supporting Oracle ILOM 3.0.

This guide is written for technicians, system administrators, authorized service providers, and users who have experience managing system hardware.

To fully understand the information that is presented in this guide, use the CLI procedures guide in conjunction with other guides in the ILOM 3.0 Documentation Collection. For a description of the guides that comprise the ILOM 3.0 Documentation Collection, see "Related Documentation" on page xv.

This preface contains the following topics:

- "Related Documentation" on page xv
- "Documentation, Support, and Training" on page xvii
- "ILOM 3.0 Version Numbers" on page xvii
- "Documentation Comments" on page xviii

Related Documentation

To fully understand the information that is presented in this guide, use this document in conjunction with the documents listed in the following table. These documents are available online at:

`http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic`

Note – The documents comprising the ILOM 3.0 Documentation Collection were formerly referred to as Sun Integrated Lights Out Manager (ILOM) 3.0 guides.

Title	Content	Part Number	Format
Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide	Information that describes ILOM features and functionality	820-6410	PDF HTML
Oracle Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide	Information and procedures for network connection, logging in to ILOM for the first time, and configuring a user account or a directory service	820-5523	PDF HTML
Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide	Information and procedures for accessing ILOM functions using the ILOM web interface	820-6411	PDF HTML
Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide	Information and procedures for accessing ILOM functions using the ILOM CLI	820-6412	PDF HTML
Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide	Information and procedures for accessing ILOM functions using SNMP or IPMI management hosts	820-6413	PDF HTML
Oracle Integrated Lights Out Manager (ILOM) 3.0 CMM Administration Guide for Sun Blade 6000 and 6048 Modular Systems	Information and procedures for managing CMM functions in ILOM.	820-0052	PDF HTML
Oracle Integrated Lights Out Manager (ILOM) 3.0 Feature Updates and Release Notes	Late breaking information about new ILOM 3.0 features, as well as known problems and work arounds.	820-7329	PDF HTML

In addition to the ILOM 3.0 Documentation Collection, associated ILOM Supplement guides or platform Administration guides present ILOM features and tasks that are specific to the server platform you are using. Use the ILOM 3.0 Documentation Collection in conjunction with the ILOM Supplement or platform Administration guide that comes with your server platform.

Translated versions of some of the guides in the ILOM Documentation Collection are available on the documentation web site. English versions of the guides in the ILOM Documentation Collection are revised more frequently and might be more up-to-date than the translated documentation.

Documentation, Support, and Training

- Documentation: `http://docs.sun.com/`
- Support: `http://www.sun.com/support/`
- Training: `http://www.sun.com/training/`

ILOM 3.0 Version Numbers

ILOM 3.0 has implemented a new version numbering scheme to help you identify which version of ILOM you are running on your system. The numbering scheme includes a five-field string, for example, `a.b.c.d.e`, where:

- `a` – Represents the major version of ILOM.
- `b` – Represents a minor version of ILOM.
- `c` – Represents the update version of ILOM.
- `d` – Represents a micro version of ILOM. Micro versions are managed per platform or group of platforms. See your platform Product Notes for details.
- `e` – Represents a nano version of ILOM. Nano versions are incremental iterations of a micro version.

For example, ILOM 3.1.2.1.a would designate:

- ILOM 3 as the major version of ILOM
- ILOM 3.1 as a minor version of ILOM 3
- ILOM 3.1.2 as the second update version of ILOM 3.1
- ILOM 3.1.2.1 as a micro version of ILOM 3.1.2
- ILOM 3.1.2.1.a as a nano version of ILOM 3.1.2.1

Documentation Comments

Submit comments about this document by clicking the Feedback[+] link at:

`http://docs.sun.com`.

Please include the title and part number of your document with your feedback:

Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide,
part number 820-6412-12

CHAPTER 1

CLI Overview

Topics

Description	Links
Supported industry-standard model for ILOM CLI	• "ILOM CLI — DMTF Server Management Command-Line Protocol User-Interface" on page 2
ILOM CLI connection requirements, installed firmware, and CLI prompt	• "ILOM CLI Connection" on page 3 • "Server SP or CMM Network Addresses Accepted by ILOM CLI" on page 3 • "ILOM CLI Firmware and CLI Prompt" on page 4
Understand ILOM CLI management namespace	• "ILOM CLI Management Namespace" on page 5 • "ILOM CLI Target Types" on page 5 • "Server SP and CMM CLI Management Targets" on page 6 • "Supported DMTF CLP Commands" on page 7 • "CLI Command Options" on page 7 • "Server SP – CLI Target Tree" on page 8
Syntax requirements and examples for executing CLI commands	• "Entering CLI Command Syntax and Executing Commands" on page 9
Quick reference for common CLI commands	• "Common CLI Commands" on page 10
Compare previous ILOM 2.0 properties with later ILOM 3.0 properties	• "ILOM 3.0 Properties Versus ILOM 2.x Properties" on page 16

Related Topics

For ILOM	Chapter or Section	Guide
• Concepts	• ILOM Overview	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide* (820-6410)
• Web interface	• Web Interface Overview	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* (820-6411)
• SNMP and IPMI hosts	• SNMP Overview • IPMI Overview	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide* (820-6413)
• Feature Updates	• New or Updated Features	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Feature Updates and Release Notes* (820-7329)

The ILOM 3.0 Documentation Collection is available at:
`http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic`

This chapter introduces the basic information you need to know before you perform procedures using the ILOM command-line interface (CLI).

ILOM CLI — DMTF Server Management Command-Line Protocol User-Interface

The ILOM CLI is based on the Distributed Management Task Force specification, *Server Management Command-Line Protocol Specification, version 11.0a.8 Draft* (DMTF CLP). You can view the entire specification at the following site:

`http://www.dmtf.org/`

The DMTF CLP provides a management user-interface for one or more servers regardless of server state, method of access, or installed operating system.

The DMTF CLP architecture models a hierarchical namespace, a predefined tree that contains every managed object in the system. In this model, a small number of commands operate on a large namespace of targets, which can be modified by options and properties. This namespace defines the targets for each command verb.

For more information about managing objects in the ILOM CLI namespace, see "ILOM CLI Management Namespace" on page 5.

ILOM CLI Connection

You can use a command-line interface to access ILOM on the chassis monitoring module (CMM) or the server service processor (SP) through a network connection, or through a direct terminal connection to the serial port on the CMM or server SP. In addition, on some Oracle Sun servers you can use the Local Interconnect Interface feature in ILOM to manage the server directly from the host operating system without any physical network or local connecton to the server.

Note – For more information about how to use the Local Interconnect Interface feature in ILOM, see the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*. For instructions about how to connect a local serial device to a server or how to connect a network cable to the NET MGT port on a server or CMM, see the Installation Guide provided with your server or CMM.

Topics discussed in this section include:

- "Server SP or CMM Network Addresses Accepted by ILOM CLI" on page 3
- "ILOM CLI Firmware and CLI Prompt" on page 4

Server SP or CMM Network Addresses Accepted by ILOM CLI

As of ILOM 3.0.12 or later, the following network addresses are accepted by the ILOM service processor (SP) CLI.

- **IPv4 address**, such as `10.8.183.106`
- **IPv6 address**, such as `fec0:a:8:b7:214:4fff:5eca:5f7e/64`
- **Link Local IPv6 address**, such as `fe80::214:4fff:feca:5f7e/64`
- **DNS host domain address**, such as `company.com`

Examples for Entering an IPv6 Address

When specifying an IPv6 address in a URL with a web browser or when transfering a file, the IPv6 address must be enclosed in brackets to work correctly. For example:

- When entering a URL in a web browser, type:

`https://[`*ipv6address***`]`**

- When transferring a file using the CLI `load -source` command and `tftp`, type:

`load -source tftp://``[`*ipv6address*`]`*filename*`.`*extension*

However, when specifying an IPv6 address to log in to ILOM using an SSH connection, the IPv6 address should **not be enclosed** in brackets. For example:

- When establishing an ILOM CLI session using SSH and the default ILOM `root` user account, type:

`ssh root@`*ipv6address*

For additional information about entering IPv6 addresses, refer to the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*. For help with diagnosing IPv4 and IPv6 connection issues, see "Diagnosing IPv4 or IPv6 ILOM Connection Issues" on page 255.

ILOM CLI Firmware and CLI Prompt

After establishing a connection to the CLI session on a server SP or a CMM, the ILOM firmware version installed on the system is identified and the copyright information and CLI prompt appears.

For example:

```
Oracle(R) Integrated Lights Out Manager

Version 3.0.0.0 r54408

Copyright (c) 2010, Oracle and/or its affiliates. All rights
reserved.

->
```

Note – As of ILOM 3.0.10, you can change the CLI prompt on the CMM to differentiate between a CMM CLI prompt and a server module (blade) CLI prompt. For more information about the new CLI prompt properties and how to make the CLI prompt specific to a CMM or a blade, see the *Oracle Integrated Lights Out Manager (ILOM) CMM Administration Guide for Sun Blade 6000 and Sun Blade 6048 Modular Systems.*

ILOM CLI Management Namespace

The ILOM CLI management namespace includes a hierarchical predefined tree that contains every managed object in the system. Within the ILOM CLI, a small number of commands operate on a large namespace of targets that are modified by options and properties.

Topics discussed in this section include:

- "ILOM CLI Target Types" on page 5
- "Server SP and CMM CLI Management Targets" on page 6
- "Supported DMTF CLP Commands" on page 7
- "CLI Command Options" on page 7
- "Server SP – CLI Target Tree" on page 8

ILOM CLI Target Types

TABLE 1-1 lists the ILOM CLI target types that you can access depending on the Oracle Sun server platform that you are using.

TABLE 1-1 ILOM Target Types

Target Type	Description
`* /SP`	The targets and properties below this target type are used for configuring the ILOM service processor (SP) and for viewing logs and consoles.
`* /CMM`	On blade platforms, this target type replaces `/SP` and is used for configuring the ILOM chassis monitoring module (CMM).
`* /SYS`	The targets and properties below this target type provide inventory, environmentals, and hardware management. The targets directly correspond to nomenclature for all hardware components, some of which are printed onto the physical hardware.
`* /CH`	On blade platforms, this target type replaces `/SYS` and provides inventory, environmentals, and hardware management at the chassis level. The target types directly correspond to nomenclature names for all hardware components, some of which are printed onto the physical hardware.
`* /HOST`	The targets and properties below this target type are used for monitoring and managing the host operating system.

Note – Access to the target types within the hierarchy depends on the Sun server platform you are using.

Server SP and CMM CLI Management Targets

From the ILOM CLI server SP, you can access the `/SP` namespace and the system namespaces which include: `/SYS` and `/HOST`. In the `/SP` namespace, you can manage and configure the service processor. In the `/SYS` or `/HOST` namespace you can access other information about the managed system hardware.

From the ILOM CLI CMM, you can access the `/CMM` namespace and the chassis component namespace, which could include: `/CH/BL`*n*, `/CH/BL`*n*`/Node`*n*, or `/CH/NEM`. In the `/CMM` namespace you can manage and configure the CMM. In the `/CH` namespaces you can access and configure properties for managed chassis componenets such as single SP server modules (blades), multiple SP server modules, and NEMs.

TABLE 1-2 identifies ILOM CLI server and CMM management targets you can navigate in ILOM.

TABLE 1-2 CMM and Server SP CLI Management Targets

ILOM Management Component	CLI Management Target Descriptions
Server SP	• `/SP` is used to configure the server module SP and for viewing logs and consoles. • `/SYS` is used to provide inventory, environmental, and hardware management at the server module level.
CMM, Chassis, and Server Module SP (blade)	• `/CMM` is used to manage ILOM on the CMM. • `/CH` is used to provide inventory, environmental, and hardware management at the chassis level. The `/CH` address space replaces `/SYS` on Sun Blade Modular Systems. • `/CH/BL`*n* is used to access and configure server module SP properties and options from the CMM CLI session . • `/CH/BL`*n*`/Node`*n* is used to access and configure properties and options on a specific SP node on a server module that supports multiple SPs.
Host	• `/HOST` is used to monitor and manage the host server operating system interactions.

Supported DMTF CLP Commands

The ILOM CLI supports the DMTF CLP commands listed in the following table.

Note – CLI commands are case-sensitive.

TABLE 1-3 CLI Commands

Command	Description
`cd`	Navigates the object namespace.
`create`	Sets up an object in the namespace.
`delete`	Removes an object from the namespace.
`exit`	Terminates a CLI session.
`help`	Displays Help information for commands and targets.
`load`	Transfers a file from an indicated source to an indicated target.
`dump`	Transfers a file from a target to a remote location specified by the URI.
`reset`	Resets the state of the target.
`set`	Sets target properties to the specified value.
`show`	Displays information about targets and properties.
`start`	Starts the target.
`stop`	Stops the target.
`version`	Displays the version of service processor running.

CLI Command Options

The ILOM CLI supports the following options, but note that not every command supports every option. The `help` option can be used with any command.

TABLE 1-4 CLI Options

Option Long Form	Short Form	Description
`-default`		Causes the command to perform its default functions only.
`-destination`		Specifies the destination for data.
`-display`	`-d`	Shows the data the user wants to display.
`-force`	`-f`	Specifies that the action will be performed immediately.

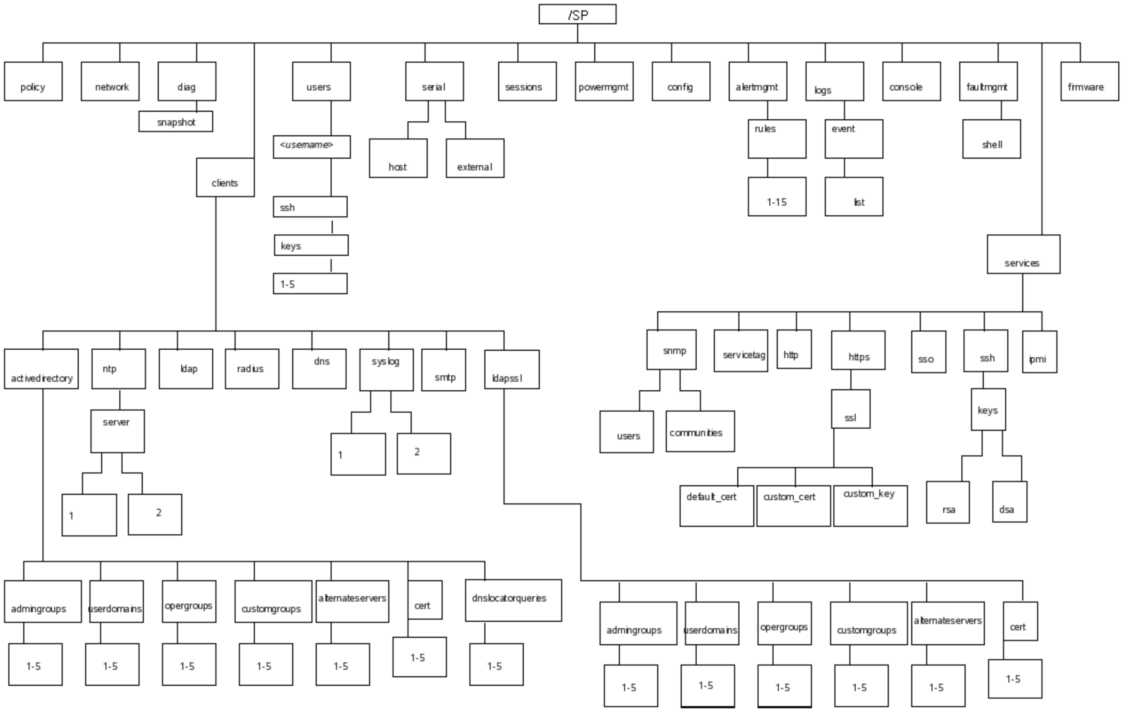
TABLE 1-4 CLI Options *(Continued)*

Option Long Form	Short Form	Description
`-help`	`-h`	Displays Help information.
`-level`	`-l`	Executes the command for the current target and all targets contained through the level specified.
`-output`	`-o`	Specifies the content and form of command output. ILOM only supports `-o table`, which displays targets and properties in tabular form.
`-script`		Skips warnings or prompts normally associated with the command.
`-source`		Indicates the location of a source image.

Server SP – CLI Target Tree

Every object in the CLI namespace is considered a target.

FIGURE 1-1 `/SP` Example of the ILOM CLI Target Tree



Entering CLI Command Syntax and Executing Commands

To specify target locations and successfully execute CLI commands in ILOM, you must apply the require command-line syntax when entering and executing commands. For more details, see the following topics:

- "Entering CLI Command Syntax" on page 9
- "Executing Commands" on page 9

Entering CLI Command Syntax

When using the ILOM CLI, information is entered in the following command syntax: **command [***options***] [***target***] [***properties***]**

For example:

```
-> set /SP/services/https port=portnumber servicestate=enabled|disabled
```

Note – Syntax examples in this chapter use the target starting with /SP/, which could be interchanged with the target starting with /CMM/ depending on your server platform. Subtargets are common across all server platforms.

Executing Commands

To execute most commands, specify the location of the target and then enter the command. You can perform these actions individually, or you can combine them on the same command line.

▼ Execute Commands Individually

1. **Navigate to the namespace using the `cd` command.**

   For example:

   ```
   cd /SP/services/http
   ```

2. Enter the command, target, and value.

For example:

```
-> set port=80
```

or

```
-> set prop1=x
-> set prop2=y
```

▼ Execute Combined Commands

- **Using the syntax** `<command><target>=`*value*, **enter the command on a single command line.**

For example:

```
-> set /SP/services/http port=80
```

or

```
-> set /SP/services/http prop1=x prop2=y
```

Common CLI Commands

Note – For more information about ILOM CLI commands, see "CLI Command Reference" on page 225.

TABLE 1-5 General Commands

Description	Command
Display information about commands and targets	**`help`**
Display information about a specific command	**`help`** <*string*>
Show all valid targets	**`help targets`**
Change and display the current target	**`cd`**
Transfer a file from a target to a remote location specified by the URI	**`dump`**
Log out of the CLI	**`exit`**
Display the version of ILOM firmware running on ILOM	**`version`**
Reset a target	**`reset`**
Display clock information	**`show /SP/clock`**

TABLE 1-5 General Commands *(Continued)*

Description	Command
Display active ILOM sessions	**show /SP/sessions**
Update ILOM and BIOS firmware	**load -source** *tftp://newSPimage*
Display a list of ILOM event logs	**show /SP/logs/event/list**

TABLE 1-6 User Commands

Description	Command
Add a local user	**create /SP/users/***user1* **password=***password* **role=a|u|c|r|o|s**
Delete a local user	**delete /SP/users/***user1*
Change a local user's properties	**set /SP/users/***user1* **role=operator**
Display information about all local users	**show -display [**targets|properties|all**] -level all /SP/users**
Display information about LDAP settings	**show /SP/clients/ldap**
Change LDAP settings	**set /SP/clients/ldap binddn=***proxyuser* **bindpw=***proxyuserpassword* **defaultrole=a|u|c|r|o|s address=***ipaddress*

TABLE 1-7 Network and Serial Port Setting Commands

Description	Command
Display network configuration information	**show /SP/network**
Change network properties for ILOM. Changing certain network properties, like the IP address, will disconnect your active session	**set /SP/network pendingipaddress=***ipaddress* **pendingipdiscovery=dhcp|static pendingipgateway=***ipgateway* **pendingipnetmask=***ipnetmask* **commitpending=true**
Display information about the external serial port	**show /SP/serial/external**

TABLE 1-7 Network and Serial Port Setting Commands *(Continued)*

Description	Command
Change the external serial port configuration	**set /SP/serial/external pendingspeed=***integer* **commitpending=true**
Display information about the serial connection to the host	**show /SP/serial/host**
Change the host serial port configuration. Note: This speed setting must match the speed setting for serial port 0, COM1, or /dev/ttyS0 on the host operating system	**set /SP/serial/host pendingspeed=***integer* **commitpending=true**

TABLE 1-8 Alert Management Commands

Description	Command
Display information about alerts. You can configure up to 15 alerts	**show /SP/alertmgmt/rules/1...15**
Configure an IPMI PET alert	**set /SP/alertmgmt/rules/1...15 type=ipmipet destination=***ipaddress* **level= down|critical|major|minor**
Configure a v3 SNMP trap alert	**set /SP/alertmgmt/rules/1...15 type=snmptrap snmp_version=3 comunity_or_username=***username* **destination=***ipaddress* **level= down|critical|major|minor**
Configure an email alert	**set /SP/alertmgmt/rules/1...15 type=email destination=***email_address* **level= down|critical|major|minor**

TABLE 1-9 System Management Access Commands

Description	Command
Display information about HTTP settings	**`show /SP/services/http`**

Change HTTP settings, such as enabling automatic redirection to HTTPS	**`set /SP/services/http port=`***portnumber*
	`secureredirect= enabled|disabled`
	`servicestate=enabled|disabled`

Display information about HTTPS access	**`show /SP/services/https`**
Change HTTPS settings	**`set /SP/services/https port=`***portnumber* **`servicestate=enabled|disabled`**
Display SSH DSA key settings	**`show /SP/services/ssh/keys/dsa`**
Display SSH RSA key settings	**`show /SP/services/ssh/keys/rsa`**

TABLE 1-10 Clock Settings Commands

Description	Command
Set ILOM clock to synchronize with a primary NTP server	**`set /SP/clients/ntp/server/1 address=`***ntpIPaddress*
Set ILOM clock to synchronize with a secondary NTP server	**`set /SP/clients/ntp/server/2 address=`***ntpIPaddress2*

TABLE 1-11 SNMP Commands

Description	Command
Display information about SNMP settings. By default, the SNMP port is 161 and v3 is enabled	**show /SP/services/snmp engineid=***snmpengineid* **port=***snmpportnumber* **sets=enabled|disabled v1=enabled|disabled v2c=enabled|disabled v3=enabled|disabled**
Display SNMP users	**show /SP/services/snmp/users**
Add an SNMP user	**create /SP/services/snmp/users/***snmpusername* **authenticationpassword=***password* **authenticationprotocol=MD5|SHA permissions=rw|ro privacypassword=***password* **privacyprotocol=none|DES**
Delete an SNMP user	**delete /SP/services/snmp/users/***snmpusername*
Display SNMP MIBs	**show /SP/services/snmp/mibs**
Display information about SNMP public (read-only) communities	**show /SP/services/snmp/communities/public**
Display information about SNMP private (read-write) communities	**show /SP/services/snmp/communities/private**
Add an SNMP public community	**create /SP/services/snmp/communities/ public/***comm1* **permission=ro|rw**
Add an SNMP private community	**create /SP/services/snmp/communities/ private/***comm2* **permission=ro|rw**
Delete an SNMP community	**delete /SP/services/snmp/communities/***comm1*

TABLE 1-12 Host System Commands

Description	Command
Start the host system or chassis power	**start /SYS** or **start /CH**
Stop the host system or chassis power (graceful shutdown)	**stop /SYS** or **stop /CH**
Stop the host system or chassis power (forced shutdown)	**stop [-f|force] /SYS** or **stop [-f|force] /CH**
Reset the host system or chassis	**reset /SYS** or **reset /CH**

TABLE 1-12 Host System Commands *(Continued)*

Description	Command
Start a session to connect to the host console	**`start /SP/console`**
Stop the session connected to the host console (graceful shutdown)	**`stop /SP/console`**
Stop the session connected to the host console (forced shutdown)	**`stop [-f|force] /SP/console`**

TABLE 1-13 Filtering Output Options for Commands

Description	Filtered Command
Display active ILOM sessions that were started on July 17th	**`show /SP/sessions -level all starttime== "*Jul 17*"`**
Display users that have admin roles	**`show /SP/users -level all role=="a*"`**
Display users that *only* have user and console roles	**`show /SP/users -level all role=="uc"`**
Display all SNMP trap alerts	**`show /SP/alertmgmt -level all type== "snmptrap"`**
Display all disabled services	**`show /SP/services -level all servicestate== disabled`**
Display NTP clients that use the NTP address server IP 1.2.3.4	**`show /SP/clients/ntp -level all address== "1.2.3.4"`**
Display all FRUs with serial number that starts with 0D01B	**`show /SYS fru_serial_number=="0D01B*" -level all`**
Display all memory modules manufactured by INFINEON	**`show /SYS -level all type=="DIMM" fru_manufacturer=="INFINEON"`**
Display all power supplies whose alarm state is major	**`show /SYS -level all type=="Power Supply" alarm_status==major`**
Display all components that are DIMMs or hard disks	**`show /SYS type==("Hard Disk",DIMM) -level all`**
Display all voltage sensors whose upper_nonrecov_threshold value is 2.89 or 60 Volts	**`show /SYS type==Voltage upper_nonrecov_threshold==("2.*","60.*")`**

ILOM 3.0 Properties Versus ILOM 2.x Properties

Note – Properties are the configurable attributes specific to each object.

If you are upgrading from ILOM 2.x to ILOM 3.0 and you want to update your 2.x scripts, you need to be familiar with the new methods that ILOM 3.0 uses to implement ILOM 3.0 commands. TABLE 1-14 lists ILOM 2.x properties and the new ILOM 3.0 implementations that replace them.

TABLE 1-14 ILOM 2.x Properties and New ILOM 3.0 Implementations

ILOM 2.x Properties	ILOM 3.0 Implementation
`/SP/clients/syslog/destination_ip1`	`/SP/clients/syslog/1/address`
`/SP/clients/syslog/destination_ip2`	`/SP/clients/syslog/2/address`
`/SP/clients/activedirectory/getcertfile` (load a certificate)	Use `load` command with this target `/SP/clients/activedirectory/cert`
`/SP/clients/activedirectory/getcertfile` (remove a certificate)	Use `set` command with `/SP/client/activedirectory/cert clear_action=true`
`/SP/clients/activedirectory/getcertfile` (restore a certificate)	No longer a feature
`/SP/clients/activedirectory/certfilestatus`	`/SP/clients/activedirectory/cert/certstatus`
`/SP/clients/activedirectory/ipaddress`	`/SP/clients/activedirectory/address`
`/SP/clients/activedirectory/alernativeservers/getcertfile` (load a certificate)	Use `load` command with `/SP/clients/activedirectory/alernativeservers/cert` as target
`/SP/clients/activedirectory/alernativeservers/getcertfile` (remove a certificate)	Use `set` command with `/SP/client/activedirectory/alernativeservers/cert clear_action=true`
`/SP/clients/activedirectory/getcertfile/alernativeservers/` (restore a certificate)	No longer a feature
`/SP/clients/activedirectory/alernativeservers/certfilestatus`	`/SP/clients/activedirectory/alernativeservers/cert/certstatus`

TABLE 1-14 ILOM 2.x Properties and New ILOM 3.0 Implementations *(Continued)*

ILOM 2.x Properties	ILOM 3.0 Implementation
/SP/clients/activedirectory/alernativeservers/ipaddress	/SP/clients/activedirectory/alernativeservers/address
/SP/clients/radius/ipaddress	/SP/clients/radius/address
/SP/clients/ldap/ipaddress	/SP/clients/ldap/address
/SP/cli/commands	Use help command with a target name
/SP/diag/state	/HOST/diag/state
/SP/diag/generate_host_nmi	/HOST/generate_host_nmi
/SP/diag/mode	/HOST/diag/mode
/SP/diag/level	/HOST/diag/level
/SP/diag/verbosity	/HOST/diag/verbosity

CHAPTER 2

Logging In to and Out of ILOM

Topics

Description	Links
Review the prerequisites	• "Before Your Initial Login" on page 20
Log in to ILOM using default user account and password	• "Log In to ILOM CLI - Using ILOM Default User Account and Password" on page 21
Set up a user account	• "Set Up a User Account" on page 22
Log in to ILOM using ILOM user name and password	• "Log In to ILOM CLI - Using ILOM User Name and Password" on page 23
Set a timeout value for a CLI session	• "Set a Timeout Value for a CLI Session" on page 23
Configure banner messages in ILOM	• "Configure Banner Messages in ILOM" on page 24
Log out of ILOM	• "Log Out of ILOM" on page 26
Recover a Lost Password	• "Recover a Lost Password" on page 26

Related Topics

For ILOM	Chapter or Section	Guide
• Getting started	• Getting Started With ILOM • Initial ILOM Setup Procedures Using the CLI	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide* (820-5523)

The ILOM 3.0 Documentation Collection is available at: `http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic`.

Related Topics

For ILOM	Chapter or Section	Guide
• Web interface	• Logging In to and Out of ILOM	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* (820-6411)

The ILOM 3.0 Documentation Collection is available at:
`http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic`.

Use this chapter as a quick reference for ILOM login and logout procedures. For additional information, refer to the initial login process and procedures in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide.*

Before Your Initial Login

Prior to performing the procedures in this chapter, ensure that the following requirements are met:

- Review the topics about establishing communication with ILOM in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide.*
- In order to communicate with ILOM, you must establish a physical serial or network management connection on the system (server SP or CMM). Or, connect to ILOM from the host operating system by using the Local Interconnect Interface feature provided on some server platforms.

  For instructions about how to connect a nework cable to the server's NET MGT port or a device to the server's SER MGT port, refer to the installation guide provided with your server or CMM. For details about how to connect to ILOM directly from the host operating system (without the need for a physical connection to the server SER MGT port or NET MGT port) , see the topic about Local Interconnect Interface in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*.
- ILOM, by default, uses DHCP to learn the IPv4 address of the server SP (or CMM) and IPv6_Stateless to learn the IPv6 address of the server SP (or CMM). If these default network settings for obtaining an IP address for the server SP (or CMM) do not apply to your network environment, you will need to modify these settings prior to logging in to ILOM. For instructions about modifying the network settings in ILOM using the CLI, see"Configuring Network Settings" on page 30.

Note – As of ILOM 3.0.12, network configuration settings for dual-stack IPv4 and IPv6 are provided. Prior to ILOM 3.0.12, network configuration settings for IPv4 are provided.

- You will need a user account and password to log in to ILOM. However, if you are the system administrator and you are logging in to ILOM for the first time, you can use default user account (root) and password (password) to log in. After logging in to ILOM for the first time, it is highly recommended that you establish new (non-root) user accounts and passwords for each ILOM user.

  For instructions about creating and managing user accounts in ILOM using the CLI, see“Managing User Accounts” on page 57.

Logging In to ILOM

Topics

Description	Links	Platform Feature Support
Log in to ILOM and set up a user account	• ”Log In to ILOM CLI - Using ILOM Default User Account and Password” on page 21 • ”Set Up a User Account” on page 22 • ”Log In to ILOM CLI - Using ILOM User Name and Password” on page 23	• x86 system server SP • SPARC system server SP • CMM
Set a timeout value for a CLI session	• ”Set a Timeout Value for a CLI Session” on page 23	

▼ Log In to ILOM CLI - Using ILOM Default User Account and Password

1. **Using a Secure Shell (SSH) session, log in to the ILOM CLI by specifying the default** `root` **user account, and IP address of the server SP or CMM.**

   For example:

   $ **`ssh root@`***system_ipaddress*

   If ILOM is operating in a dual-stack network environment, the *system_ipaddress* can be entered using either an IPv4 or IPv6 address format. For example,

- IPv4 address format: `10.8.183.106`

or

- IPv6 address format: `fec0:a:8:b7:214:4fff:5eca:5f7e/64`

  For more information about entering IP addresses in a dual-stack environment, see "Server SP or CMM Network Addresses Accepted by ILOM CLI" on page 3. For help with diagnosing IPv4 and IPv6 connection issues, see "Diagnosing IPv4 or IPv6 ILOM Connection Issues" on page 255.

The system prompts you for a password.

2. **Type** `changeme` **as the default password.**

   For example:

   ```
   Password: changeme
   ```

   The ILOM CLI prompt appears (->).

Note – As of ILOM 3.0.4, you can set the amount of time a CLI session can remain idle before the session times out and closes. For instructions, see "Set a Timeout Value for a CLI Session" on page 23.

▼ Set Up a User Account

After you have logged in to ILOM, you need to create a regular (non-`root`) user account.

To set up a user account, follow this step:

- **Set up a user account in one of these five classes of users:**
  - Local users
  - Active Directory users
  - LDAP users
  - LDAP/SSL users
  - RADIUS users

You can create up to 10 local user accounts or configure a directory service. For information about setting up a user account, see "Managing User Accounts" on page 57.

▼ Log In to ILOM CLI - Using ILOM User Name and Password

Note – Use this procedure to log in to ILOM to verify that the user account or directory service is functioning properly.

---

1. **Using a Secure Shell (SSH) session, log in to ILOM by specifying your user name and IP address of the server SP or CMM.**

   For example:

   ```
   $ ssh username@ipaddress
   ```

   The system prompts you for your ILOM password.

2. **Type your ILOM password.**

   ```
   Password: password
   ```

   The ILOM CLI prompt appears (->).

▼ Set a Timeout Value for a CLI Session

Note – The Admin (a) role is required to change the `cli timeout` configuration variable. You must be using ILOM 3.0.4 or a later version of ILOM.

---

1. **Log in to the ILOM SP CLI or the CMM CLI.**

2. **To view the current settings, type:**

   ```
   -> show /SP/cli
   ```

3. **To set the timeout value, type the following command:**

   ```
   -> set /SP/cli timeout=n
   ```

   Where *n* is a number between 0 and 1440.

Note – 0 (zero) indicates that the CLI session timeout is disabled, so that the CLI session will not close regardless of the amount of time the session is idle.

For example, to set the timeout value to 60 minutes, type:

```
-> set /SP/cli timeout=60
Set ‘timeout’ to ‘60’
```

Configuring Banner Messages

Topics

Description	Links	Platform Feature Support
Review the prerequisites	• "Before You Begin" on page 24	• x86 system server SP • SPARC system server SP • CMM
Configure banner messages in ILOM	• "Configure Banner Messages in ILOM" on page 24	

Before You Begin

- The Admin (a) role is required to configure banner messages in ILOM.
- You must be using ILOM 3.0.8 or a later version of ILOM.

▼ Configure Banner Messages in ILOM

1. **Log in to the ILOM SP CLI or the CMM CLI.**
2. **Use the `show` command to display the current banner properties and supported commands.**

   For example:

```
-> show /SP/preferences/banner

/SP/preferences/banner
    Targets:

    Properties:
        connect_message = (none)
        login_message = (none)
        login_message_acceptance = disabled

    Commands:
        cd
        set
        show
```

3. **To create a banner message, perform any of the following tasks:**

Task	Instructions
To create a banner message to appear on the Login page	Type: `-> set /SP/preferences/banner connect_message=`*message* Where *message* equals the content you want to appear on the Login page.
To create banner message to appear in a dialog box after logging in to ILOM.	Type: `-> set /SP/preferences/banner login_message=`*message* Where *message* equals the content you want to appear after logging in to ILOM.

Note - Messages are limited to a 1000 characters. To create a new line within the message, use the following CLI characters: `/r` or `/n`.

4. **To enable the system to display the banner messages, type:**

```
-> set /SP/preferences/banner/ login_message_acceptance=enabled
```

5. **To disable the system from displaying the banner messages type:**

```
-> set /SP/preferences/banner/ login_message_acceptance=disabled
```

Logging Out of ILOM and Recovering a Lost Password

Topics

Description	Links	Platform Feature Support
Log out of ILOM	• ”Log Out of ILOM” on page 26	• x86 system server SP • SPARC system server SP • CMM
Recover a lost password	• ”Recover a Lost Password” on page 26	

Log Out of ILOM

To log out of ILOM, follow this step:

- **At the command prompt, type:**

```
-> exit
```

Recover a Lost Password

Before You Begin

- You must be physically present at the server to perform this procedure.

You can use the preconfigured `default` user account to recover a lost password or to re-create the `root` user account. For more information about the `root` and `default` user accounts, refer to "`root` and `default` User Accounts" in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide.*

To recover a lost password, follow these steps:

1. **Log in to an ILOM serial console using the** `default` **user account.**

   For example:

   ```
   SUNSP-0000000000 login: default
   Press and release the physical presence button.
   Press return when this is completed...
   ```

2. **Prove physical presence at your server.**

   Refer to your platform documentation for instructions on how to prove physical presence.

3. **Return to your serial console and press Enter.**

   You will be prompted for a password.

4. **Type the password for the** `default` **user account:** **`defaultpassword`**

Note – It is recommended that you reset your password at this time. See "Change a User Account Password" on page 60.

What Next

After you have logged in to ILOM and set up a user account, you are now ready to configure settings for ILOM functions. The remaining chapters in the Oracle ILOM 3.0 CLI Procedures Guide provide descriptions of the tasks you can perform to access ILOM functions.

CHAPTER 3

Configuring ILOM Communication Settings

Topics

Description	Links
Configure network settings	• ”View and Configure IPv4 Network Settings” on page 32 • ”Edit Existing IPv4 Addresses in ILOM” on page 34 • ”View and Configure Dual-Stack IPv4 and IPv6 Network Settings” on page 35 • ”Test IPv4 or IPv6 Network Configuration” on page 40 • ”Assign Host Name and System Identifier” on page 41 • ”View and Configure DNS Settings” on page 42 • ”View and Configure Serial Port Settings” on page 43 • ”Enable HTTP or HTTPS Web Access” on page 44 • ”Switch Serial Port Output” on page 46
Configure Secure Shell settings	• ”Establish a Secure Remote SSH Connection” on page 47 • ”Enable or Disable SSH” on page 47 • ”View the Current Key” on page 48 • ”Generate a New SSH Key” on page 49 • ”Restart the SSH Server” on page 50
Configure the Local Interconnect Interface	• ”Configure the Local Interconnect Interface” on page 52

Related Topics

For ILOM	Chapter or Section	Guide
• Concepts	• ILOM Network Configurations	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide* (820-6410)
• Getting started	• Connecting Your System to ILOM	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide* (820-5523)
• Web interface	• Configuring ILOM Communication Settings	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* (820-6411)
• IPMI and SNMP hosts	• Configuring ILOM Communication Settings	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide* (820-6413)

The ILOM 3.0 Documentation Collection is available at: `http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic`.

Configuring Network Settings

Topics

Description	Links	Platform Feature Support
Review the prerequisites	• "Before You Begin" on page 31	• x86 system server SP • SPARC system server SP • CMM
View and configure IPv4 network settings	• "View and Configure IPv4 Network Settings" on page 32	
Edit existing IPv4 addresses	• "Edit Existing IPv4 Addresses in ILOM" on page 34	
View and configure dual-stack IPv4 and IPv4 network settings	• "View and Configure Dual-Stack IPv4 and IPv6 Network Settings" on page 35	
Test IPv4 or IPv6 network configuration	• "Test IPv4 or IPv6 Network Configuration" on page 40	

Topics

Description	Links	Platform Feature Support
Assign a host name and system identifier	• ”Assign Host Name and System Identifier” on page 41	• x86 system server SP • SPARC system server SP • CMM
View and configure DNS settings	• ”View and Configure DNS Settings” on page 42	
View and configure serial port settings	• ”View and Configure Serial Port Settings” on page 43	
Enable HTTP or HTTPS web access	• ”Enable HTTP or HTTPS Web Access” on page 44	
Switch serial port output between the SP console and the host console	• ”Switch Serial Port Output” on page 46	• x86 system server SP

Before You Begin

Review the following information before you view or configure ILOM network settings.

Network Environment	Before You Begin
IPv4-only	• To configure network settings, you need the Admin (a) role enabled. • Prior to configuring ILOM communication settings, ensure that the same IP address is always assigned to ILOM by either assigning a static IP address to ILOM after initial setup, or by configuring your DHCP server to always assign the same IP address to ILOM. This enables ILOM to be easily located on the network. By default, ILOM will attempt to obtain network settings using DHCP.
Dual-stack IPv4 and IPv6	• To configure or test network settings, you need the Admin (a) role enabled. • Verify that your server or CMM has ILOM firmware 3.0.12 or later installed. • Verify that support for the IPv6 configuration options in either your platform ILOM Supplement guide or platform Administration guide. • Review the IPv6 enhancements identified in Chapter 2 of the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide* (820-6410).

Network Environment	Before You Begin
	• ILOM supports a dual-mode TCP/IP stack and is shipped from the factory with both the IPv4 and IPv6 states enabled by default. If necessary, you can optionally disable the IPv6 network state. However, the IPv4 network state must always be enabled in order for ILOM to operate in an IPv4 network environment or in a dual-stack IPv4 and IPv6 network environment. • ILOM supports static and DHCP network settings for both IPv4 and IPv6 network environments. • For IPv6 Stateless auto-configurations, ILOM (3.0.12 or later) requires a network router to be configured for IPv6. • For DHCPv6 auto-configuration options, ILOM (3.0.14 or later) requires a network DHCPv6 server to provide the IPv6 address(es) and DNS information for the device. **Note -** DHCP and DHCPv6 are separate protocols. In a dual-stack network environment, DHCP and DHCPv6 operate as follows: (1) the DHCPv6 server can provide IPv6 addresses to a network node and the network node always uses the IPv6 protocol to communicate with a DHCPv6 server; and (2) the DHCP server can provide IPv4 addresses to a network node and the network node will always use the IPv4 protocol to communicate with a DHCP server • For DHCP and DHCPv6 auto-configurations, you should choose to receive the DNS information from either an IPv6 DHCP server or from an IPv4 DHCP server, but not from both. You can manually configure the settings for the DNS Name Server in ILOM under the Network DNS target. For instructions on specifying DNS information, see "View and Configure DNS Settings" on page 42.
Other network settings described in this section	• You need to have the Admin (a) role enabled to modify any server SP or CMM network properties or options.

▼ View and Configure IPv4 Network Settings

Note – This procedure provides instructions for configuring ILOM to operate in an IPv4-only network environment, as is supported in ILOM 3.0.10 and earlier versions of ILOM. If you are configuring ILOM to operate in an dual-stack IPv4 and IPv6 network environment, see "View and Configure Dual-Stack IPv4 and IPv6 Network Settings" on page 35.

---

1. **Log in to the ILOM SP CLI or the CMM CLI.**

2. **At the command prompt, type:**

```
-> show /SP/network
```

3. **Use the `set` command and type all of the settings that you wish to change.**

   You can execute these commands within a combined command. See "Execute Combined Commands" on page 10.

Note – Change a complete set of properties and commit to `true` only when the pending values are all typed into the command.

Note – Settings take effect as soon you set `commitpending=true`. Configuring network settings might disconnect your active session if you are connected to ILOM over a network. Configure all your systems before you commit the changes. After you commit the changes you will have to reconnect to ILOM.

Example

To change multiple network settings from DHCP to static assigned settings, type:

```
-> set /SP/network pendingipdiscovery=static pendingipaddress=
nnn.nn.nn.nn pendingipgateway=nnn.nn.nn.nn pendingipnetmask=nnn.nn.nn.nn
commitpending=true
```

Targets, Properties, and Values

The following target, properties, and values are valid for ILOM network settings.

TABLE 3-1 ILOM Target, Properties, and Values for Network Settings

Target	Property	Value	Default

`/SP/network`	`ipaddress`
	`ipdiscovery`
	`ipgateway`
	`ipnetmask`
		Read-only; values are updated by the system	

	`macaddress`	MAC address of ILOM	
	`commitpending`	`true|none`	`none`
	`pendingipaddress`	<*ipaddress*|`none`>	`none`
	`pendingipdiscovery`	`dhcp|static`	`dhcp`
	`pendingipgateway`	<*ipaddress*|`none`>	`none`
	`pendingipnetmask`	<*ipdotteddecimal*>	`255.255.255.0`
	`dhcp_server_ip`	Read-only; value is updated when the SP receives a DHCP address	
	`state`	`enabled|disabled`	`none`

▼ Edit Existing IPv4 Addresses in ILOM

1. **Log in to the ILOM SP CLI or the CMM CLI.**

2. **Type one of the following commands to set the SP working directory:**
   - For a rackmount standalone server: `cd /SP/network`
   - For a chassis server blade server module: `cd /SP/network`
   - For a chassis CMM: `cd /CMM/network`

3. **Type the `show` command to view the IP address assigned.**

4. **Type the following commands to change the existing settings.**

Command	Description and Example
`set pendingipaddress=` *<ipaddress>*	Type this command followed by the static IP address that you want to assign to the server SP or CMM.
`set pendingipnetmask=` *<ipnetmask>*	Type this command followed by the static Netmask address that you want to assign to the server SP or CMM.
`set pendingipgateway=` *<ipgateway>*	Type this command followed by the static Gateway address that you want to assign to the server SP or CMM.
`set pendingipdiscovery=` *<ipdiscovery>*	Type this command to set a static IP address on the server SP or CMM.

`set commitpending=true`	Type this command to assign the network settings specified.
	
	For example:
	`set pendingipaddress=129.144.82.26`
	`set pendingipnetmask=255.255.255.0`
	`set pendingipgateway=129.144.82.254`
	`set pendingipdiscovery=static`
	`set commitpending=true`

Note – If you connected to ILOM through a remote SSH connection, the connection made to ILOM using the former IP address will timeout. Use the newly assigned settings to connect to ILOM.

▼ View and Configure Dual-Stack IPv4 and IPv6 Network Settings

---

Note – This procedure provides instructions for configuring ILOM to operate in a dual-stack IPv4 and IPv6 network environment. If you are configuring ILOM to operate in an IPv4-only network environment, as is supported in ILOM 3.0.10 and earlier versions of ILOM, see "View and Configure IPv4 Network Settings" on page 32.

---

1. **Log in to the ILOM SP CLI or the CMM CLI.**

   Establish a local serial console connection or SSH connection to the server SP or CMM.

2. **Perform the network configuration instructions that apply to your network environment:**

   - To configure IPv4 network settings, perform Step 3 to Step 5 in this procedure.
   - To configure IPv6 network settings, perform Step 6 to Step 10 in this procedure.

3. **For IPv4 network configurations, use the `cd` command to navigate to the `/`*`x`*`/network` working directory for the device.**

   For example:

   - For a rackmount server SP type: `cd /SP/network`
   - For a chassis CMM type: `cd /CMM/network`
   - For a chassis blade server SP type: `cd /CH/BL`*`n`*`/network`
   - For a chassis blade server with multiple SP nodes type: `cd /CH/BL`*`n`*`/Node`*`n`*`/network`

4. **Type the `show` command to view the configured IPv4 network settings configured on the device.**

5. **To set IPv4 network settings for DHCP or static, perform one of the following:**

- **To configure DHCP IPv4 network settings**, set values for the following properties:

Property	Set Property Value	Description
`state`	`set state=enabled`	The network `state` is `enabled` by default for IPv4. **Note -** To enable the DHCP network option for IPv4 the `state` must be set to `enabled`.
`pendingipdiscovery`	`set pendingipdiscovery=dhcp`	The property value for `ipdiscovery` is set to `dhcp` by default for IPv4. **Note -** If the `dhcp` default property value was changed to `static`, you will need to set the property value to `dhcp`.
`commitpending=`	`set commitpending=true`	Type `set commitpending=true` to commit the changes made to the `state` and `ipdiscovery` property values.

- **To configure static IPv4 network settings**, set values for the following properties:

Property	Set Property Value	Description
`state`	`set state=enabled`	The network `state` is `enabled` by default for IPv4. **Note -** To enable the static IPv4 network option the `state` must be set to `enabled`.
`pendingipdiscovery`	`set pendingipdiscovery=static`	To enable a static IPv4 network configuration, you need to set the `pendingipdiscovery` property value to `static`. **Note -** The property value for `ipdiscovery` is set to `dhcp` by default for IPv4.

`pendingipaddress`
`pendingipnetmask`
`pendingipgateway`
	`set pendingipaddress=` <*ip_address*> `pendingipnetmask=` <*netmask*> `pendingipgateway=` <*gateway*>	To assign multiple static network settings, type the `set` command followed by the `pending` command for the each property value (IP address, netmask, and gateway), then type the static value that you want to assign.

`commitpending=`	`set commitpending=true`	Type `set commitpending=true` to commit the changes madeto the IPv4 network properties.

6. **For IPv6 network configurations, use the `cd` command to navigate to the `/`*x*`/network/ipv6` working directory for the device.**

   For example:

   - For a rackmount server SP type: `cd /SP/network/ipv6`
   - For a chassis CMM type: `cd /CMM/network/ipv6`
   - For a chassis blade server SP type: `cd /CH/BL`*n*`/network/ipv6`
   - For a chassis blade server with multiple SP nodes type: `cd /CH/BL`*n*`/Node`*n*`/network/ipv6`

7. **Type the `show` command to view the configured IPv6 network settings configured on the device.**

   For example, see the following sample output values for the IPv6 properties on a server SP device.

```
-> show

 /SP/network/ipv6
    Targets:

    Properties:
        state = enabled
        autoconfig = stateless
        dhcpv6_server_duid = (none)
        link_local_ipaddress = fe80::214:4fff:feca:5f7e/64
        static_ipaddress = ::/128
        ipgateway = fe80::211:5dff:febe:5000/128
        pending_static_ipaddress = ::/128
        dynamic_ipaddress_1 = fec0:a:8:b7:214:4fff:feca:5f7e/64

    Commands:
        cd
        show
```

Note – When the `autoconfig=` property is set to `dhcpv6_stateful` or `dhcpv6_stateless`, the read-only property for `dhcpv6_server_duid` will identify the DHCP Unique ID of the DHCPv6 server that was last used by ILOM to retrieve the DHCP information.

Note – The default IPv6 autoconfig property value provided in ILOM 3.0.14 (and later) is autoconfig=stateless. However, if you have ILOM 3.0.12 installed on your CMM or server, the default property value for autoconfig appears as autoconfig=stateless_only.

8. **To configure an IPv6 auto-configuration option, use the set command to specify the following auto-configuration property values.**

Property	Set Property Value	Description
state	set state=enabled	The IPv6 network state is enabled by default. To enable an IPv6 auto-configuration option this state must be set to enabled.
autoconfig	set autoconfig=<*value*>	Specify this command followed by the autoconf value you want to set. Options include: • stateless (default setting provided in ILOM 3.0.14 or later) *or* stateless_only (default setting provided in ILOM 3.0.12) Automatically assigns IP address learned from the IPv6 network router. • dhcpv6_stateless Automatically assigns DNS information learned from the DHCP server. The dhcpv6_stateless property value is available in ILOM as of 3.0.14. • dhcpv6_stateful Automatically assigns the IPv6 address learned from the DHCPv6 server. The dhcpv6_stateful property value is available in ILOM as of 3.0.14. • disable Disables all auto-configuration property values and sets the read-only property value for link local address.

Note – The IPv6 configuration options take affect after they are set. You do not need to commit these changes under the /network target.

Note – IPv6 auto-configuration addresses learned for the device will not affect any of the active ILOM sessions to the device. You can verify the newly learned auto-configured addresses under the `/network/ipv6` target.

Note – As of ILOM 3.0.14 or later, you can enable the `stateless` auto-configuration option to run at the same time as when the option for `dhcpv6_stateless` is enabled or as when the option for `dhcpv6_stateful` is enabled. However, the auto-configuration options for `dhcpv6_stateless` and `dhcpv6_stateful` should not be enabled to run at the same time.

---

9. **Perform the following steps to set a static IPv6 address:**

   a. **To set a pending static IPv6 address, specify the following property values:**

Property	Set Property Value	Description
`state`	`set state=enabled`	The IPv6 network state is `enabled` by default. To enable a static IP address this state must be set to `enabled`.
`pendingipaddress`	`set pending_static_ipaddress=` *<ip6_address>*/*<subnet mask length in bits>*	Type this command followed by the property value for the static IPv6 address and net mask that you want to assign to the device. IPv6 address example: `fec0:a:8:b7:214:4fff:feca:5f7e/64`

   b. **To commit (save) the pending IPv6 static network parameters, perform the steps in the following table:**

Step	Description
1	Use the `cd` command to change the directory to the device `network` target. For example: • For rackmount server type: `cd /SP/network` • For chassis CMM type: `cd /CMM/network` • For chassis blade server SP type: `cd /CH/BL`*n*`/network` • For chassis blade server SP with multiple nodes type: `cd /CH/BL`*n*`/Node`*n*`/network`
2	Type the following command to commit the changed property values for IPv6: `set commitpending=true`

Note – Assigning a new static IP address to the device (SP or CMM) will end all active ILOM sessions to the device. To log back in to ILOM, you will need to create a new browser session using the newly assigned IP address.

10. **To test the IPv4 or IPv6 network configuration from ILOM use the Network Test Tools (Ping and Ping6). For details, see** ”Test IPv4 or IPv6 Network Configuration” on page 40**.**

Test IPv4 or IPv6 Network Configuration

1. **Log in to the ILOM SP CLI or the CMM CLI.**

   Establish a local serial console connection or SSH connection to the server SP or CMM

2. **Use the** `cd` **command to navigate to the** /*x*/network/test **working directory for the device, for example:**

   - For a rackmount server SP type: `cd /SP/network/test`
   - For a chassis CMM type: `cd /CMM/network/test`
   - For a chassis blade server SP type: cd /CH/BL*n*/network/test
   - For a chassis blade server with multiple SP nodes type: cd /CH/BL*n*/Node*n*/network/test

3. **Type the** `show` **command to view the network** `test` **targets and properties.**

   For example, see the following output the shows the test target properties on a CMM device.

```
-> show

/CMM/network/test
   Targets:

   Properties:
       ping = (Cannot show property)
       ping6 = (Cannot show property)

   Commands:
       cd
       set
       show
```

4. **Use the** `set ping` **or** `set ping6` **command to send a network test from the device to a specified network destination.**

Property	Set Property Value	Description
`ping`	`set ping=`<*IPv4_address*>	Type the `set ping=` command at the command prompt followed by the IPv4 test destination address. For example: -> `set ping=10.8.183.106` `Ping of 10.8.183.106 succeeded`
`ping6`	`set ping6=`<*IPv6_address*>	Type the `set ping6=` command followed by the IPv6 test destination address. For example: -> `set ping6=fe80::211:5dff:febe:5000` `Ping of fe80::211:5dff:febe:5000 succeeded`

Assign Host Name and System Identifier

1. **Log in to the ILOM SP CLI or the CMM CLI.**

2. **To set the SP host name and system identifier text, at the command prompt, type:**

   -> **`set /SP hostname=`***text_string*

   -> **`set /SP system_identifier=`***text_string*

   Where:

   - The host name can consist of alphanumeric characters and can include hyphens. Host names can contain up to 60 characters.
   - The system identifier can consist of a text string using any standard keyboard keys except quotation marks.

   For example:

   -> **`set /SP hostname=Lab2-System1`**

   -> **`set /SP system_identifier=DocSystemforTesting`**

   With these settings, the `show` command produces the following output:

```
-> show /SP
/SP
    Targets:
          alertmgmt
          .
```

```
           .
           .
           users
    Properties:
           check_physical_presence = false
           hostname = Lab2-System1
           system_contact = (none)
           system_description = SUN BLADE X8400 SERVER MODULE, ILOM
              v3.0.0.0, r31470
           system_identifier = DocSystemforTesting
           system_location = (none)
   Commands:
           cd
           reset
           set
           show
           version
```

View and Configure DNS Settings

1. **Log in to the ILOM SP CLI or the CMM CLI.**

2. **At the command prompt type the following command to display settings for the external serial port:**

   -> **`cd /SP/clients/dns`**

3. **Use the** `set` **command to change properties and values for DNS settings. At the command prompt type:**

   `->` **`set /SP/clients/dns [propertyname=`*`value`*`]`**

   For example:

   `->` **`set /SP/clients/dns searchpath=`**`abcdefg.com`

Targets, Properties, and Values

The following targets, properties, and values are valid for DNS settings.

TABLE 3-2 Valid Targets, Properties, and Values for DNS Settings

Target	Property	Value	Default
`/SP/clients/dns`	`auto_dns`	`enabled|disabled`	`disabled`
	`nameserver`	*ip_address*	
	`retries`	Integer between 0 and 4	
	`searchpath`	Integer between 1 and 10	
	`timeout`	Up to six comma-separated search suffixes	

View and Configure Serial Port Settings

1. **Log in to the ILOM SP CLI or the CMM CLI.**
2. **At the command prompt:**
   - Type the following command to display settings for the external serial port:

     ```
     -> show /SP/serial/external
     ```

   - Type the following command to display settings for the host serial port:

     ```
     -> show /SP/serial/host
     ```

3. **Use the** `set` **command to change properties and values for serial port settings. Port settings have two sets of properties: pending and active. At the command prompt type:**

   ```
   -> set target [propertyname=value] commitpending=true
   ```

Example

To change the speed (baud rate) for the host serial port from 9600 to 57600, type the following:

- For x86-based systems

  ```
  -> set /SP/serial/host pendingspeed=57600 commitpending=true
  ```

- For SPARC-based systems

  ```
  -> set /SP/serial/external pendingspeed=57600 commitpending=true
  ```

Note – On x86-based systems, the speed of the host serial port must match the speed setting for serial port 0, COM1, or /dev/ttys0 on the host operating system for ILOM to communicate properly with the host.

Targets, Properties, and Values

The following targets, properties, and values are valid for ILOM serial port settings.

TABLE 3-3 Valid Targets, Properties, and Values for ILOM Serial Port Settings

Target	Property	Value	Default
`/SP/serial/external`	`commitpending`	`true|(none)`	`(none)`
	`flowcontrol`	`software`	`software`
	`pendingspeed`	*<integer>*	`9600`
	`speed`	Read-only value; configured via the `pendingspeed` property	
`/SP/serial/host`	`commitpending`	`true|(none)`	`(none)`
	`pendingspeed`	*<integer>*	`(none)`
	`speed`	Read-only value; configured via the `pendingspeed` property	

▼ Enable HTTP or HTTPS Web Access

1. **Log in to the ILOM SP CLI or the CMM CLI.**
2. **At the command prompt, type:**

```
-> set /SP/services/http [propertyname=value]
```

The properties are located in `/SP/services/http` and `/SP/services/https`.

Targets, Properties, and Values

TABLE 3-4 shows the valid targets, properties, and values for HTTP and HTTPS connections.

TABLE 3-4 Valid Targets, Properties, and Values for HTTP and HTTPS Connections

Target	Property	Value	Default
`/SP/services/http`	`secureredirect`	`enabled|` `disabled`	`enabled`
	`servicestate`	`enabled|` `disabled`	`disabled`
	`port`	*<portnum>*	`80`
`/SP/services/https`	`servicestate`	`enabled|` `disabled`	`enabled`
	`port`	*<portnum>*	`443`

TABLE 3-5 lists the possible settings for HTTP, HTTPS, and automatic redirect.

TABLE 3-5 Possible Settings for HTTP, HTTPS, and Automatic Redirect

Desired State	Target	Property	Value
Enable HTTP only	`/SP/services/http`	`secureredirect`	`disabled`
	`/SP/services/http`	`servicestate`	`enabled`
	`/SP/services/https`	`servicestate`	`disabled`
Enable HTTP and HTTPS	`/SP/services/http`	`secureredirect`	`disabled`
	`/SP/services/http`	`servicestate`	`enabled`
	`/SP/services/https`	`servicestate`	`enabled`
Enable HTTPS only	`/SP/services/http`	`secureredirect`	`disabled`
	`/SP/services/http`	`servicestate`	`disabled`
	`/SP/services/https`	`servicestate`	`enabled`
Automatically redirect HTTP to HTTPS	`/SP/services/http`	`secureredirect`	`enabled`
	`/SP/services/http`	`servicestate`	`disabled`
	`/SP/services/https`	`servicestate`	`enabled`

▼ Switch Serial Port Output

Note – To determine whether serial port sharing is supported for your server, refer to the platform ILOM Supplement guide or platform Administration guide provided for your server.

Caution – You should set up the network on the SP before attempting to switch the serial port owner to the host server. If a network is not set up, and you switch the serial port owner to the host server, you will be unable to connect using the CLI or web interface to change the serial port owner back to the SP. To return the serial port owner setting to the SP, you will need to restore access to the serial port on the server. For more details about restoring access to the server port on your server, see the platform documentation supplied with your server.

---

1. **Log in to the ILOM SP CLI.**

2. **To set the serial port owner, type:**

```
-> set /SP/serial/portsharing /owner=host
```

Note – The serial port sharing value by default is `owner=SP`.

---

3. **Use a dongle or multi-port cable to connect a serial host to the server.**

   For details on how to use aattach devices to the server, see the platform installation documentation supplied with your server.

Configuring Secure Shell Settings

Topics

Description	Links	Platform Feature Support
Configure Secure Shell settings	• ”Establish a Secure Remote SSH Connection” on page 47 • ”Enable or Disable SSH” on page 47 • ”View the Current Key” on page 48 • ”Generate a New SSH Key” on page 49 • ”Restart the SSH Server” on page 50	• x86 system server SP • SPARC system server SP • CMM

Before You Begin

- To configure Secure Shell (SSH) settings, you need the Admin (a) role enabled.

▼ Establish a Secure Remote SSH Connection

● **You will need to establish a secure connection from a remote SSH client to the server SP. To establish a secure connection, type the following:**

```
$ ssh -l username server_ipaddress
Password: ********
```

The default CLI prompt appears and the system is ready for you to run the CLI commands to establish network settings.

▼ Enable or Disable SSH

Note – SSH is enabled by default in ILOM.

Follow these steps to enable or disable SSH:

1. **Log in to the ILOM SP CLI or the CMM CLI.**
2. **If you do not want to provide access over the network, or if you do not want to use SSH, type the following:**

   `-> set /SP/services/ssh state=`*enabled* | *disabled*

▼ View the Current Key

Note – All of the properties below `/SP/services/ssh/keys/`*rsa*|*dsa* are read only. To view the key, you need the Read Only (`o`) role enabled.

Follow one of these steps to view the current key:

- **To view the RSA key, type:**

```
-> show /SP/services/ssh/keys/rsa
    For example:
/SP/services/ssh/keys/rsa
    Targets:
       Properties:
          fingerprint =
ca:c0:05:ff:b7:75:15:a0:30:df:1b:a1:76:bd:fe:e5
          length = 1024
           publickey
AAAAB3NzaC1yc2EAAAABIwAAAIEAthvlqgXbPIxN4OEvkukKupdFPr8GDaOsKGg
BESVlnny4nX8yd8JC/hrw3qDHmXIZ8JAFwoLQgjtZCbEsgpn9nNIMb6nSfu6Y1t
TtUZXSGFBZ48ROmU0SqqfR3i3bgDUR0siphlpgV6Yu0Zd1h3549wQ+RWk3vxqHQ
Ffzhv9c=
      Commands:
          cd
          show
```

- **To view the DSA key, type:**

```
-> show /SP/services/ssh/keys/dsa
For example:
 /SP/services/ssh/keys/dsa
     Targets:

     Properties:
        fingerprint =
6a:90:c7:37:89:e6:73:23:45:ff:d6:8e:e7:57:2a:60
        length = 1024
        publickey =
AAAAB3NzaC1kc3MAAACBAInrYecNH86imBbUqE+3FoUfm/fei2ZZtQzqrMx5zBm
bHFIaFdRQKeoQ7gqjc9jQbO7ajLxwk2vZzkg3ntnmqHz/hwHvdho2KaolBtAFGc
fLIdzGVxi4I3phVb6anmTlbqI2AILAa7JvQ8dEGbyATYR9A/pf5VTac/TQ70O/J
AAAAFQCIUavkex7wtEhC0CH3s25ON0I3CwAAAIBNfHUop6ZN7i46ZuQOKhD7Mkj
gdHy+8MTBkupVfXqfRE9Zw9yrBZCNsoD8XEeIeyP+puO5k5dJvkzqSqrTVoAXyY
qewyZMFE7stutugw/XEmyjq+XqBWaiOAQskdiMVnHa3MSg8PKJyWP8eIMxD3rIu
PTzkV632uBxzwSwfAQAAAIAtA8/3odDJUprnxLgHTowc8ksGBj/wJDgPfpGGJHB
B1FDBMhSsRbwh6Z+s/gAf1f+S67HJBTUPsVSMz+czmamc1oZeOazT4+zeNG6uCl
u/5/JmJSdkguc1FcoxtBFqfO/fKjyR0ecWaU7L4kjvWoSsydHJ0pMHasEecEBEr
lg==

     Commands:
         cd
         show
```

Generate a New SSH Key

Follow these steps to generate a new SSH key:

1. **Log in to the ILOM SP CLI or the CMM CLI.**

2. **Set the key type by typing the following:**

   `-> set /SP/services/ssh generate_new_key_type=`*dsa*|*rsa*

3. **Set the action to** `true`.

   ```
   -> set /SP/services/ssh generate_new_key_action=true
   ```

   The fingerprint and key will look different. The new key will take effect immediately for new connections.

▼ Restart the SSH Server

Note – Restarting the SSH server will end any existing SSH connections.

Follow these steps to restart the SSH server:

1. **Log in to the ILOM SP CLI or the CMM CLI.**
2. **To restart the SSH server, type the following:**

```
-> set /SP/services/ssh restart_sshd_action=true
```

Configuring the Local Interconnect Interface

Topics

Description	Links	Platform Feature Support
Review the prerequisites	• "Before You Begin" on page 50	• x86 system server SP • SPARC system server SP
Configure the Local Interconnect Interface	• "Configure the Local Interconnect Interface" on page 52	

Before You Begin

The following requirements must be met before performing the procedures described in this section for configuring the Local Interconnect Interface in ILOM.

- Review the concepts describing the use of a Local Interconnect Interface between the ILOM SP and the host OS. For details, see "Local Interconnect Interface: Local Connection to ILOM From Host Operating System" in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*.
- Review the ILOM descriptions for the Local Host Interconnect configuration settings. For details, see "Local Host Interconnect Configuration Settings in ILOM" in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*.
- Verify that your server is running ILOM 3.0.12 or a later version of ILOM.

- Verify that your platform supports the Local Interconnect Interface. Refer to your platform server ILOM Supplement guide or Administration guide.

Note – The settings in ILOM for the Local Interconnect Interface are not supported on the CMM.

- Automatic configuration of the Local Interconnect Interface requires the `Host Managed` (`hostmanaged`) setting in ILOM to be enabled (set to `True`), as well as the installation of the Oracle Hardware Management Pack 2.1.0 or later software on the server. For more information about installing the Oracle Hardware Management Pack 2.1.0 software, see the *Oracle Server Hardware Management Pack User's Guide* (821-1609).
- Manual configuration of the Local Interconnect Interface between the ILOM SP and the host operating system requires the Host Managed (`hostmanaged`) setting in ILOM to be disabled (set to `False`), as well as other configuration settings to be set on the host operating system.

  For guidelines for configuring the host OS connection point on the Local Interconnect Interface, see "Manual Host OS Configuration Guidelines for Local Interconnect Interface" on page 257.
- The host operating system must support the internal USB Ethernet device that is presented from the ILOM SP. Therefore, prior to configuring the Local Interconnect Interface in ILOM, you should verify that an internal USB Ethernet device driver was included in the operating system distribution and installed on your server. If an internal USB Ethernet device driver was not installed by the operating system distribution, you can obtain the device driver for your operating system from the Oracle Hardware Management Pack 2.1.0 software. For more details, see the *Oracle Server Hardware Management Pack User's Guide* (821-1609).
- Network parameter changes to the settings in ILOM for the Local Interconnect Interface are considered pending until you commit the changes in the ILOM. For example, in the ILOM CLI, you must issue the `commitpending=true` command to save the `pendingipaddress` and the `pendingipnetmask` under the `network/interconnect` target. In the ILOM web interface, network parameter changes entered on the Configure USB Ethernet Parameters dialog are committed after clicking `Save`.
- An ILOM user account with Administrator (a) role privileges is required in order to change any of the settings in ILOM for the Local Interconnect Interface.
- To determine the operating systems supported on your server, refer to the platform server installation guide or operating system guide(s).

▼ Configure the Local Interconnect Interface

1. **Log in to the ILOM SP CLI.**

   Establish a local serial console connection or SSH connection to the server SP or CMM

2. **Use the `cd` command to navigate to the `/`*x*`/network/interconnect` working directory for the server.**

   For example:

   - For a rackmount server SP type: `cd /SP/network/interconnect`
   - For a chassis blade server SP type: `cd /CH/BL`*n*`/network/interconnect`

3. **Type the `show` command to view the network `interconnect` targets and properties.**

   Example outputs:

   - `hostmanaged` property under the `network/interconnect` property is set to `true`. In this configuration example, the host managed state is enabled for auto-configuration by the Oracle Hardware Management Pack 2.1.0 or later software.

```
-> show

/SP/network/interconnect
    Targets:
Properties:
        hostmanaged = true
        type = USB Ethernet
        ipaddress = 169.254.182.76
        ipnetmask = 255.255.255.0
        spmacaddress = 02:21:28:57:47:16
        hostmacaddress = 02:21:28:57:47:17
Commands:
        cd
        set
        show
```

- hostmanaged property under the network/interconnect property is set to false. In this configuration example, the host managed state is disabled allowing you to manually configure the ILOM SP and host OS connection points on the Local Interconnect Interface.

```
-> show

 /SP/network/interconnect
    Targets:
Properties:
        hostmanaged = false
        state = enabled
        type = USB Ethernet
        ipaddress = 169.254.182.76
        ipnetmask = 255.255.255.0
        spmacaddress = 02:21:28:57:47:16
        hostmacaddress = 02:21:28:57:47:17
        pendingipaddress = 169.254.182.76
        pendingipnetmask = 255.255.255.0
        commitpending = (Cannot show property)
Commands:
        cd
        set
        show
```

4. **To configure the assignment of the non-routable IPv4 addresses to the connection points on the Local Interconnect Interface, you can choose to:**

   - Automatically assign non-routable IPv4 addresses to each connection point on the Local Interconnect Interface by setting the hostmanaged property to true.

     ```
     -> set hostmanaged=true
     ```

     When you set the hostmanaged property to true, you must also install the Oracle Hardware Management Pack 2.1.0 (or later) software on your server and accept the installation default for enabling Local ILOM Interconnect. For more information, see the section about configuring the Local ILOM Interconnect in the *Oracle Server Hardware Management Pack User's Guide* (821-1609).

   - or-

   - Manually assign non-routable IPv4 addresses to each connection point on the Local Interconnect Interface by setting the hostmanaged property to false.

```
-> set hostmanaged=false
```

When you set the `hostmanaged` property to `false`, you must also manually set the values for the following `/network/interconnect` properties.

Property	Set Property Value	Description
`state`	`set state=enabled`	Type `set state=enabled` to manually enable the Local Interconnect Interface between the ILOM SP and host OS. The `state` property under the `interconnect` target is `disabled` by default.
`pendingipaddress`	`set pendingipaddress= 169.254.182.76`	ILOM, by default, provides a non-routable IPv4 address for the ILOM SP connection point on the Local Interconnect Interface. This default IPv4 address (169.254.182.76) should not be changed unless a conflict exists on the host OS with this IPv4 address. To change the default IPv4 address, type the `set pendingipaddress=` command followed by the internal IPv4 address that you want to assign to the ILOM SP connection point on the Local Interconnect Interface.
`pendingipnetmask`	`set pendingipnetmask= 255.255.255.0`	ILOM, by default, provides an IPv4 Netmask address for the ILOM SP connection point on the Local Interconnect Interface. This default IPv4 Netmask (255.255.255.0) address should not be changed unless a conflict exists in your network environment with this address. To change the default Netmask address, type the `set pendingipnetmask=` command follow by the internal IPv4 Netmask that you want to assign to the ILOM SP connection point on the Local Interconnect Interface.

`commitpending`	`set commitpending=`<*value*>	Changes under the `network/interconnect` target for both `pendingipaddress` and `pendingipnetmask` are considered pending until they are committed.
		To commit the changes, type:
		`set commitpending=true`
		To cancel the changes, type:
		`set commitpending=false`

For additional information about the values required for the manual local host interconnect configuration properties, type `help`. For example:

```
-> help hostmanaged
-> help state
-> help pendingipaddresss
->help pendingipnetmask
->help commitpending
```

For additional information about the read-only properties, type:

```
-> help type
-> help ipaddress
-> help ipnetmask
-> help spmacaddress
-> help hostmacaddress
```

If you chose to manually configure the Local Interconnect Interface in ILOM without the use of the Oracle Hardware Management Pack 2.1.0 software, you will need to perform some additional configuration on the host operating system. For general details about these additional host OS configuration settings, see "Manual Host OS Configuration Guidelines for Local Interconnect Interface" on page 257.

Note – To prevent the Oracle Hardware Management Pack software from auto-configuring the connection points on the Local Interconnect Interface, the `hostmanaged` property value must be set to `False`. To prevent the use of Local Interconnect Interface between the ILOM SP and the host OS, the `state` property value must be set to `disabled` and the `hostmanaged` property value must be set to `False.`

CHAPTER 4

Managing User Accounts

Topics

Description	Links
Configure user accounts	• ″Configure Single Sign On″ on page 59 • ″Add a User Account″ on page 60 • ″Change a User Account Password″ on page 60 • ″Assign Roles to a User Account″ on page 61 • ″Delete a User Account″ on page 61 • ″View Individual User Accounts″ on page 62 • ″View a List of User Accounts″ on page 63 • ″View a List of User Sessions″ on page 63 • ″View an Individual User Session″ on page 64
Configure SSH user key	• ″Add an SSH Key″ on page 65 • ″Delete an SSH Key″ on page 65
Configure Active Directory settings	• ″Enable Active Directory `strictcertmode`″ on page 67 • ″Check Active Directory `certstatus`″ on page 67 • ″Remove an Active Directory Certificate″ on page 69 • ″View and Configure Active Directory Settings″ on page 69 • ″Troubleshoot Active Directory Authentication and Authorization″ on page 78
Configure LDAP settings	• ″Configure the LDAP Server″ on page 79 • ″Configure ILOM for LDAP″ on page 80

Topics

Description	Links
Configure LDAP/SSL settings	• "Enable LDAP/SSL `strictcertmode`" on page 82 • "Check LDAP/SSL `certstatus`" on page 82 • "Remove an LDAP/SSL Certificate" on page 83 • "View and Configure LDAP/SSL Settings" on page 84 • "Troubleshoot LDAP/SSL Authentication and Authorization" on page 90
Configure RADIUS settings	• "Configure RADIUS" on page 92

Related Topics

For ILOM	Chapter or Section	Guide
• Concepts	• User Account Management • Guidelines for Managing User Accounts	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide* (820-6410)
• Web interface	• Managing User Accounts	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide.* (820-6411)
• IPMI and SNMP hosts	• Managing User Accounts	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide* (820-6413)
The ILOM 3.0 Documentation Collection is available at: `http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic`.		

Note – Syntax examples in this chapter use the target starting with `/SP/`, which could be interchanged with the target starting with `/CMM/` depending on your Oracle server platform. Subtargets are common across all Oracle Sun server platforms.

Configuring User Accounts

Topics

Description	Links	Platform Feature Support
Configure user accounts	• ”Configure Single Sign On” on page 59 • ”Add a User Account” on page 60 • ”Assign Roles to a User Account” on page 61 • ”Delete a User Account” on page 61 • ”View a List of User Accounts” on page 63 • ”View an Individual User Session” on page 64 • ”View a List of User Sessions” on page 63 • ”View an Individual User Session” on page 64	• x86 system server SP • SPARC system server SP • CMM

Before You Begin

- To disable or enable Single Sign On, you need the Admin (a) role enabled.
- To add or edit user account properties or assign roles, you need the User Management (u) role enabled.

▼ Configure Single Sign On

1. **Log in to the ILOM SP CLI or the CMM CLI.**
2. **To enable or disable Single Sign On, type the following command:**

```
-> set /SP/services/sso state=disabled|enabled
```

▼ Add a User Account

1. **Log in to the ILOM SP CLI or the CMM CLI.**

2. **To add a local user account, type the following command:**

   ```
   -> create /SP/users/username password=password
   ```

   For example:

```
-> create /SP/users/user5
Creating user...
Enter new password: ********
Enter new password again: ********
Created /SP/users/user5
```

Note – When adding a user account, it is unnecessary to provide a role or password property. The role will default to Read Only (o), and the CLI will prompt you to provide and confirm a password.

▼ Change a User Account Password

1. **Log in to the ILOM SP CLI or the CMM CLI.**

2. **To change a user account password, type the following command:**

   ```
   -> set /SP/users/user password
   ```

   For example:

```
-> set /SP/users/user5 password
Enter new password: ********
Enter new password again: ********
```

Assign Roles to a User Account

1. **Log in to the ILOM SP CLI or the CMM CLI.**

2. **To assign roles to a user account, type the following command:**

   —> set /SP/users/<_username_> **password=**<_password_> **role=** <_administrator_|_operator_|_a_|_u_|_c_|_r_|_o_|_s_>

   For example:

```
-> set /SP/users/user5 role=auc
Set 'role' to 'auc'-> show /SP/users/user5
/SP/users/user5
Targets:
ssh

Properties:
role = auco
password = ********

Commands:
cd
set
show
```

Delete a User Account

1. **Log in to the ILOM SP CLI or the CMM CLI.**

2. **To delete a local user account, type the following command:**

   —> delete /SP/users/_username_

   For example:

```
-> delete /SP/users/user5
```

3. **When queried, type** `y` **to delete, or** `n` **to cancel.**

   For example:

```
Are you sure you want to delete /SP/users/user5 (y/n)? y

Deleted /SP/users/user5
```

View Individual User Accounts

1. **Log in to the ILOM SP CLI or the CMM CLI.**

2. **To display information about one specific user account, type the following command:**

   -> show /SP/users/*username*

   For example:

```
-> show /SP/users/user1

 /SP/users/user1
    Targets:
        ssh

    Properties:
        role = aucros
        password = *****

    Commands:
        cd
        set
        show
```

▼ View a List of User Accounts

1. **Log in to the ILOM SP CLI or the CMM CLI.**

2. **To display information about all local user accounts, type the following command:**

   ```
   -> show /SP/users
   ```

   For example:

```
 -> show /SP/users
  /SP/users
      Targets:
            user1
            user2
            user3
            user4
```

▼ View a List of User Sessions

1. **Log in to the ILOM SP CLI or the CMM CLI.**

2. **To display information about all local user sessions, type the following command:**

   ```
   -> show /SP/sessions
   ```

   For example:

```
-> show /SP/sessions

 /SP/sessions
    Targets:
        12 (current)

    Properties:

    Commands:
        cd
        show
```

View an Individual User Session

Note – To view an individual user's role, you must be using ILOM 3.0.4 or a later version of ILOM.

1. **Log in to the ILOM SP CLI or the CMM CLI.**
2. **To display information about an individual user session, type the following command:**

   –> show /SP/sessions/*session_number*

   For example:

```
 -> show /SP/sessions/12

  /SP/sessions/12
     Targets:

     Properties:
         username = user4
         role = aucro
         starttime = Mon Apr 13 06:25:19 2009
         type = shell
         mode = normal

     Commands:
         cd
         show
```

Configuring SSH User Keys

Topics

Description	Links	Platform Feature Support
Configure SSH user key	• "Add an SSH Key" on page 65 • "Delete an SSH Key" on page 65	• x86 system server SP • SPARC system server SP • CMM

Before You Begin

- To configure other users SSH keys, you need to have the User Management (u) role enabled. However, you can configure your own SSH key with Read-Only (o) role privileges.

The SSH keys enable you to automate password authentication. Use the following procedures in this section to add and delete SSH keys.

▼ Add an SSH Key

1. **Log in to the ILOM SP CLI or the CMM CLI.**

2. **To change to the directory location of a user's SSH key, type:**

   -> **cd /SP/users/user1/ssh/keys/1**

3. **To add a key to the user's account, type:**

   -> **set load_uri=**
   transfer_method://*username:password*@*ipaddress_or_hostname*/*directorypath*/*filename*

   Where:

   - *transfer_method* can be tftp, ftp, sftp, scp, http, or https.
   - *username* is the name of the user account on the remote system. (*username* is required for scp, sftp, and ftp. *username* is not used for tftp, and is optional for http and https.)
   - *password* is the password for the user account on the remote system. (*password* is required for scp, sftp, and ftp. *password* is not used for tftp, and is optional for http and https.)
   - *ipaddress_or_hostname* is the IP address or the host name of the remote system.
   - *directorypath* is the location of the SSH key on the remote system.
   - *filename* is the name assigned to the SSH key file.

   For example:

```
-> set load_uri=scp://adminuser:userpswd@1.2.3.4/keys/sshkey_1.pub
Set 'load_uri' to 'scp://adminuser:userpswd@1.2.3.4/keys/sshkey_1.pub'
```

▼ Delete an SSH Key

1. **Log in to the ILOM SP CLI or the CMM CLI.**

2. **To change to the directory location of a user's SSH key, type:**

```
-> cd /SP/users/user1/ssh/keys/1
```

3. **To delete a key from the user's account, type:**

```
-> set clear_action=true
```

The following confirmation prompt appears:

```
Are you sure you want to clear /SP/users/user1/ssh/keys/1
(y/n)?
```

4. **Type y.**

The SSH key is deleted and the following message appears to confirm the deletion.

```
Set 'clear_action' to 'true'
```

Configuring Active Directory

Topics

Description	Links	Platform Feature Support
Configure Active Directory settings	• "Enable Active Directory strictcertmode" on page 67 • "Check Active Directory certstatus" on page 67 • "Remove an Active Directory Certificate" on page 69 • "View and Configure Active Directory Settings" on page 69 • "Troubleshoot Active Directory Authentication and Authorization" on page 78	• x86 system server SP • SPARC system server SP • CMM

Before You Begin

- To configure Active Directory settings, you need the User Management (u) role enabled.

▼ Enable Active Directory strictcertmode

Note – By default, `strictcertmode` is disabled. When this variable is disabled, the channel is secure, but limited validation of the certificate is performed. If `strictcertmode` is enabled, then the server's certificate must have already been uploaded to the server so that the certificate signatures can be validated when the server certificate is presented.

1. **Log in to the ILOM SP CLI or the CMM CLI.**
2. **Type the following path to access the Active Directory certificate settings:**

   `->cd /SP/clients/activedirectory/cert`

3. **To load a certificate, type the following:**

   `-> set load_uri=tftp://`*IP address***/***file-path***/***filename*

Note – You can use TFTP, FTP, or SCP to load a certificate. Alternatively, you can load a SSL certificate for Active Directory using the `load -source` command from anywhere on the CLI. For example:
`-> load -source` *URI_to_SSL_certificate target*

4. **To enable** `strictcertmode`**, type the following:**

   `-> set strictcertmode=enabled`

Note – Data is always protected, even if `strictcertmode` is disabled.

▼ Check Active Directory certstatus

Note – `certstatus` is an operational variable that should reflect the current certificate state. Neither is required to exist if `strictcertmode` is disabled. However, for the `strictcertmode` to be enabled, a certificate must be loaded.

1. **Log in to the ILOM SP CLI or the CMM CLI.**

2. **To check the status of the certificate, type the following:**

   `-> show /SP/clients/activedirectory/cert`

   For example:

```
-> show /SP/clients/activedirectory/cert
   Targets:

   Properties:
       certstatus = certificate present
       clear_action = (none)
       issuer = /DC=com/DC=oracle/DC=east/DC=sales/CN=CAforActiveDirectory
       load_uri = (none)
       serial_number = 08:f3:2e:c0:8c:12:cd:bb:4e:7e:82:23:c4:0d:22:60
       subject = /DC=com/DC=oracle/DC=east/DC=sales/CN=CAforActiveDirectory
       valid_from = Oct 25 22:18:26 2006 GMT
       valid_until = Oct 25 22:18:26 2011 GMT
       version = 3 (0x02)

   Commands:
       cd
       load
       reset
       set
       show
```

▼ Remove an Active Directory Certificate

Note – The Authentication Server Certificate can be removed only when `strictcertmode` is disabled.

---

1. **Log in to the ILOM SP CLI or the CMM CLI.**
2. **Type the following:**

   ```
   -> cd /SP/clients/activedirectory/cert
   ```

3. **To remove a certificate, type one of the following commands:**
   - **`-> set clear_action=true`**
   - -> **`reset`** <*target*>

   For example:

   ```
   -> reset /SP/clients/activedirectory/cert
   ```

4. **Confirm whether you want to remove the certificate by typing `y` or `n` in response to the on-screen query.**

   The existing certificate file that had been uploaded will be removed.

▼ View and Configure Active Directory Settings

1. **Log in to the ILOM SP CLI or the CMM CLI.**
2. **Use the `show` and `set` commands to view and modify the active directory properties:**
   - **To view and modify information in the `admingroups` target:**

```
-> show /SP/clients/activedirectory/admingroups/n
```

Where *n* can be 1 to 5.

For example:

```
-> show /SP/clients/activedirectory/admingroups/1

/SP/clients/activedirectory/admingroups/1

   Targets:

Properties: name = CN=SpSuperAdmin,OU=Groups,DC=sales,
DC=east,DC=oracle,DC=com
```

Then use the `set` command to modify properties.

For example:

```
-> set /SP/clients/activedirectory/admingroups/1/ name=CN=
spSuperAdmin,OU=Groups,DC=sales,DC=oracle,DC=com
Set 'name' to 'CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle,
DC=com'
```

- **To view and modify information in the** `opergroups` **target:**

```
-> show /SP/clients/activedirectory/opergroups/1
```

For example:

```
-> show /SP/clients/activedirectory/opergroups/1

/SP/clients/activedirectory/opergroups/1

   Targets:

Properties: name = CN=SpSuperOper,OU=Groups,DC=sales,
DC=east,DC=oracle,DC=com
```

Then use the `set` command to modify properties.

For example:

```
-> set /SP/clients/activedirectory/opergroups/1 name=CN=
spSuperOper,OU=Groups,DC=sales,DC=oracle,DC=com
Set 'name' to 'CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC=com'
```

- **To view and modify information in the** `customgroups` **target:**

-> show /SP/clients/activedirectory/customgroups/1

For example:

```
-> show /SP/clients/activedirectory/customgroups/1
/SP/clients/activedirectory/customgroups/1
    Targets:

    Properties:
        name = custom_group_1
        roles = aucro
```

Then use the `set` command to modify properties.

For example:

```
-> set /SP/clients/activedirectory/customgroups/1 name=CN=
spSuperCust,OU=Groups,DC=sales,DC=oracle,DC=com
Set 'name' to 'CN=spSuperCust,OU=Groups,DC=sales,DC=oracle,DC=com'
-> set /SP/clients/activedirectory/customgroups/1 roles=au
Set 'roles' to 'au'
```

- **To view and modify information in the** `userdomains` **target:**

  -> show /SP/clients/activedirectory/userdomains/1

  For example:

```
-> show /SP/clients/activedirectory/userdomains/1
/SP/clients/activedirectory/userdomains/1
   Targets:

   Properties:
       domain = <USERNAME>@sales.example.oracle.com
```

Then use the `set` command to modify properties.

For example:

```
-> set /SP/clients/activedirectory/userdomains/1 domain=
<USERNAME>@sales.example.oracle.com
Set 'domain' to '<username>@sales.example.oracle.com'
```

Note – In the example above, `<USERNAME>` will be replaced with the user's login name. During authentication, the user's login name replaces `<USERNAME>`. Names can take the form of Fully Qualified Distinguished Name (FQDN), `domain\name` (NT), or Simple Name.

- **To view and modify information in the `alternateservers` target:**

  `-> show /SP/clients/activedirectory/alternateservers/1`

  For example:

```
-> show /SP/clients/activedirectory/alternateservers/1
/SP/clients/activedirectory/alternateservers/1
    Targets:
        cert

    Properties:
        address = 10.8.168.99
        port = 0
```

Note – The `address` property can either be the IP address or DNS (host name). If using DNS, DNS must be enabled. For more information on enabling DNS, see "View and Configure DNS Settings" on page 42.

Then use the `set` command to modify properties.

For example:

```
-> set /SP/clients/activedirectory/alternateservers/1 port=636
```

You can also use the `show` command to view the alternate server certificate information.

For example:

```
-> show /SP/clients/activedirectory/alternateservers/1/cert
 /SP/clients/activedirectory/alternateservers/1/cert
    Targets:

Properties:
        certstatus = certificate present
        clear_action = (none)
        issuer = /DC=com/DC=oracle/DC=east/DC=sales/CN CAforActiveDirectory
        load_uri = (none)
        serial_number = 08:f3:2e:c0:8c:12:cd:bb:4e:7e:82:23:c4:0d:22:60
        subject = /DC=com/DC=oracle/DC=east/DC=sales/CN=CAforActiveDirectory
        valid_from = Oct 25 22:18:26 2006 GMT
        valid_until = Oct 25 22:18:26 2011 GMT
        version = 3 (0x02)
```

Type the following to copy a certificate for an alternate server:

-> cd /SP/clients/activedirectory/alternateservers/1

-> set load_uri=
*<tftp|ftp|scp>:[//<username:password>***]@//***<ipAddress|HostName>***/***<filePath>***/**
<fileName>

The following is an example of a certificate copied using tftp:

```
-> set load_uri=tftp://10.8.172.152/sales/cert.cert
Set 'load_uri' to 'tftp://10.8.172.152/sales/cert.cert'
```

Note – The TFTP transfer method does not require a user name and password.

The following is an example of a certificate copied using ftp:

```
-> set load_uri=
ftp://sales:XpasswordX@129.148.185.50/8275_put/cert.cert
Set ’load_uri’ to
’ftp://sales:XpasswordX@129.148.185.50/8275_put/cert.cert’
```

The following is an example of a certificate copied using scp:

```
> set
load_uri=
scp://sales:XpasswordX@129.148.185.50/home/dc150698/8275_put/cert
.cert
```

Type the following to remove a certificate for an alternate server:

```
-> cd /SP/clients/activedirectory/alternateservers/1
-> set clear_action=true
```

For example:

```
-> set clear_action=true
Are you sure you want to clear /SP/clients/activedirectory/cert
(y/n)? y
Set ’clear_action’ to ’true’
```

- **To view and modify information in the** `dnslocatorqueries` **target:**

```
-> show /SP/clients/activedirectory/dnslocatorqueries/1
```

For example:

```
-> show /SP/clients/activedirectory/dnslocatorqueries/1
/SP/clients/activedirectory/dnslocatorqueries/1
    Targets:

    Properties:
        service = _ldap._tcp.gc._msdcs.<DOMAIN>.<PORT:3269>

    Commands:
        cd
        set
        show
```

Note – DNS and DNS Locator Mode must be enabled for DNS Locator Queries to work. For information about enabling DNS, see "View and Configure DNS Settings" on page 42.

The DNS Locator service query identifies the named DNS service. The port ID is generally part of the record, but it can be overridden by using the format `<PORT:636>`. Also, named services specific for the domain being authenticated can be specified by using the `<DOMAIN>` substitution marker.

Then use the `set` command to modify properties in the `dnslocatorqueries` target:

For example:

```
-> set /SP/clients/activedirectory/dnslocatorqueries/1 service=<string>
```

- **To view and modify the `expsearchmode` property:**

Note – To view and configure the `expsearchmode` property, you must be using ILOM 3.0.4 or a later.

```
-> show /SP/clients/activedirectory
```

For example:

```
-> show /SP/clients/activedirectory

 /SP/clients/activedirectory
    Targets:
        admingroups
        alternateservers
        cert
        customgroups
        dnslocatorqueries
        opergroups
        userdomains
Properties:
        address = 0.0.0.0
        defaultrole = (none)
        dnslocatormode = disabled
        expsearchmode = disabled
        logdetail = none
        port = 0
        state = disabled
        strictcertmode = disabled
        strictcredentialerrormode = disabled
        timeout = 4


 Commands:
        cd
        set
        show
```

Then use the `set` command to enable or disable the property.

For example:

```
-> set /SP/clients/activedirectory expsearchmode=enabled
Set 'expsearchmode' to 'enabled'
```

- **To view and modify the** `strictcredentialerrormode` **property:**

Note – As of ILOM 3.0.10, the `strictcredentialalerrormode` is available to control how user credential errors are processed. If this mode is enabled, a credential error reported from any server fails those user credentials. When the mode is disabled (default setting), the credentials can be presented to other servers for authentication.

```
-> show /SP/clients/activedirectory
```

For example:

```
-> show /SP/clients/activedirectory

 /SP/clients/activedirectory
    Targets:
        admingroups
        alternateservers
        cert
        customgroups
        dnslocatorqueries
        opergroups
        userdomains



Properties:
        address = 0.0.0.0
        defaultrole = (none)
        dnslocatormode = disabled
        expsearchmode = disabled
        logdetail = none
        port = 0
        state = disabled
        strictcertmode = disabled
        strictcredentialerrormode = disabled
        timeout = 4
Commands:
        cd
        set
        show
```

Then use the `set` command to enable or disable the property.

For example:

```
-> set /SP/clients/activedirectory strictcredentialerrormode=
enabled
Set 'strictcredentialerrormode' to 'enabled'
```

▼ Troubleshoot Active Directory Authentication and Authorization

1. **Log in to the ILOM SP CLI or the CMM CLI.**
2. **Type the following commands:**

   ```
   -> cd /SP/clients/activedirectory
   /SP/clients/activedirectory
   ```

   ```
   -> set logdetail=trace
   Set 'logdetail' to 'trace'
   ```

3. **Perform another authorization attempt by logging out, then logging back in to the ILOM CLI and typing the following command:**

   ```
   -> show /SP/logs/event/list Class==(ActDir) Type==(Log) Severity==
   (Trace)
   ```

   For example:

```
-> show /SP/logs/event/list Class==(ActDir) Type==(Log)

ID     Date/Time                 Class     Type      Severity
-----  ------------------------  --------  --------  --------
26     Thu Jul 10 09:40:46 2008  ActDir    Log       minor
       (ActDir)  authentication status: auth-OK
25     Thu Jul 10 09:40:46 2008  ActDir    Log       minor
       (ActDir)  server-authenticate: auth-success idx 100/0 dns-
server 10.8.143       .231
24     Thu Jul 10 09:40:46 2008  ActDir    Log       debug
       (ActDir)   custRoles
23     Thu Jul 10 09:40:46 2008  ActDir    Log       debug
       (ActDir)   role-name administrator
```

For more information on configuring event log detail, see "View and Clear the ILOM Event Log" on page 106.

Configuring Lightweight Directory Access Protocol

Topics

Description	Links	Platform Feature Support
Configure LDAP settings	• "Configure the LDAP Server" on page 79 • "Configure ILOM for LDAP" on page 80	• x86 system server SP • SPARC system server SP • CMM

Before You Begin

- To configure LDAP settings, you need the User Management (u) role enabled.

▼ Configure the LDAP Server

1. **Ensure that all users authenticating to ILOM have passwords stored in "crypt" format or the GNU extension to crypt, commonly referred to as "MD5 crypt."**

   ILOM only supports LDAP authentication for passwords stored in these two variations of the crypt format.

   For example:
   `userPassword: {CRYPT}ajCa2He4PJhNo`
   or
   `userPassword: {CRYPT}$1$pzKng1$du1Bf0NWBjh9t3FbUgf46.`

2. **Add object classes `posixAccount` and `shadowAccount`, and populate the required property values for this schema (RFC 2307).**

Required Property	Description
uid	User name for logging in to ILOM
uidNumber	Any unique number
gidNumber	Any unique number

Required Property	Description
userPassword	Password
homeDirectory	Any value (this property is ignored by ILOM)
loginShell	Any value (this property is ignored by ILOM)

3. **Configure the LDAP server to enable LDAP server access to ILOM user accounts.**

   Either enable your LDAP server to accept anonymous binds, or create a proxy user on your LDAP server that has read-only access to all user accounts that will authenticate through ILOM.

   See your LDAP server documentation for more details.

▼ Configure ILOM for LDAP

1. **Log in to the ILOM SP CLI or the CMM CLI.**

2. **Enter the proxy user name and password. Type:**

```
-> set /SP/clients/ldap binddn="cn=proxyuser, ou=people, ou=sales,
dc=oracle, dc=com" bindpw=password
```

3. **Enter the IP address of the LDAP server. Type:**

```
-> set /SP/clients/ldap address=ldapipaddress | DNS name
```

Note – If using a DNS name, DNS must be configured and functioning.

4. **Assign the port used to communicate with the LDAP server; the default port is 389. Type:**

```
-> set /SP/clients/ldap port=ldapport
```

5. **Enter the Distinguished Name of the branch of your LDAP tree that contains users and groups. Type, for example:**

```
-> set /SP/clients/ldap searchbase="ou=people, ou=sales,
dc=oracle, dc=com"
```

   This is the location in your LDAP tree that you want to search for user authentication.

6. **Set the state of the LDAP service to enabled. Type:**

```
-> set /SP/clients/ldap state=enabled
```

7. **To verify that LDAP authentication works, log in to ILOM using an LDAP user name and password.**

Note – ILOM searches local users before LDAP users. If an LDAP user name exists as a local user, ILOM uses the local account for authentication.

Configuring LDAP/SSL

Topics

Description	**Links**	**Platform Feature Support**
Configure LDAP/SSL settings	• "Enable LDAP/SSL `strictcertmode`" on page 82 • "Check LDAP/SSL `certstatus`" on page 82 • "Remove an LDAP/SSL Certificate" on page 83 • "View and Configure LDAP/SSL Settings" on page 84 • "Troubleshoot LDAP/SSL Authentication and Authorization" on page 90	• x86 system server SP • SPARC system server SP • CMM

Before You Begin

- To configure LDAP/SSL settings, you need the User Management (u) role enabled.

▼ Enable LDAP/SSL `strictcertmode`

Note – By default, `strictcertmode` is disabled. When this variable is disabled, the channel is secure, but limited validation of the certificate is performed. If `strictcertmode` is enabled, then the server's certificate must have already been uploaded to the server so that the certificate signatures can be validated when the server certificate is presented.

---

1. **Log in to the ILOM SP CLI or the CMM CLI.**

2. **Type the following path to access the LDAP/SSL certificate settings:**

   ```
   -> cd /SP/clients/ldapssl/cert
   ```

3. **To load a certificate, type the following:**

   -> set load_uri=tftp://*IP address***/***file-path***/***filename*

Note – You can use TFTP, FTP, or SCP to load a certificate.

---

4. **To enable** `strictcertmode`**, type the following:**

   ```
   -> set strictcertmode=enabled
   ```

▼ Check LDAP/SSL `certstatus`

Note – `certstatus` is an operational variable that should reflect the current certificate state of the certificate if `strictcertmode` is disabled. However, for the `strictcertmode` to be enabled, a certificate must be loaded.

---

1. **Log in to the ILOM SP CLI or the CMM CLI.**

2. **To check the status of the certificate, type the following:**

   `-> show /SP/clients/ldapssl/cert`

   For example:

```
-> show /SP/clients/ldapssl/cert

Targets:

Properties:
        certstatus = certificate present
        clear_action = (none)
issuer = /C=US/O=Entrust PKI Demonstration Cerificates
        load_uri = (none)
        serial_number = 08:f23:2e:c0:8c:12:cd:bb:4e:7e:82:23:c4:0d:22:60
        subject = /C=US/O=Entrust PKI Demonstration Cerificates/OU=Entrust/Web
Connector/OU=No Liability as per http://freecerts.entrust
        valid_from = Oct 25 22:18:26 2006 GMT
        valid_until = Oct 25 22:18:26 2011 GMT
        version = 3 (0x02)
```

Remove an LDAP/SSL Certificate

Note – The Authentication Server Certificate can only be removed when `strictcertmode` is disabled.

1. **Log in to the ILOM SP CLI or the CMM CLI.**
2. **Type the following:**

   `-> cd /SP/clients/ldapssl/cert`

3. **To remove a certificate, type the following:**

   `-> set clear_action=true`

4. **Confirm whether you want to remove the certificate by typing `y` (yes) or `n` (no) in response to the on-screen query.**

   The existing certificate file that had been uploaded will be removed.

▼ View and Configure LDAP/SSL Settings

Note – To view and configure the `optionalUserMapping` target, you must be using ILOM 3.0.4 or a later version of ILOM.

---

1. **Log in to the ILOM SP CLI or the CMM CLI.**
2. **Use the `show` and `set` commands to view and modify properties.**
   - **To view and modify information in the `admingroups` target:**

     `-> show /SP/clients/ldapssl/admingroups/`*n*

     Where *n* can be 1 to 5.

     For example:

```
-> show /SP/clients/ldapssl/admingroups/1

/SP/clients/ldapssl/admingroups/1

   Targets:

Properties: name = CN=SpSuperAdmin,OU=Groups,DC=sales,DC=
east,DC=oracle,DC=com
```

Then use the `set` command to modify properties.

For example:

```
-> set /SP/clients/ldapssl/admingroups/1/ name=CN=
spSuperAdmin,OU=Groups,DC=sales,DC=oracle,DC=com
Set 'name' to 'CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle,
DC=com'
```

- **To view and modify information in the `opergroups` target:**

```
-> show /SP/clients/ldapssl/opergroups/1
```

For example:

```
-> show /SP/clients/ldapssl/opergroups/1

/SP/clients/ldapssl/opergroups/1

   Targets:

Properties: name = CN=SpSuperOper,OU=Groups,DC=sales,DC=
east,DC=oracle,DC=com
```

Then use the `set` command to modify properties.

For example:

```
-> set /SP/clients/ldapssl/opergroups/1 name=CN=spSuperOper,OU=
Groups,DC=sales,DC=oracle,DC=com
Set 'name' to 'CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC=com'
```

- **To view and modify information in the `customgroups` target:**

  `-> show /SP/clients/ldapssl/customgroups/1`

  For example:

```
 /SP/clients/ldapssl/customgroups/1
    Targets:

    Properties:
        name = <fully qualified distinguished name only>
        roles = (none)

    Commands:
        cd
        set
        show
```

  Then use the `set` command to modify properties.

  For example:

```
-> set /SP/clients/ldapssl/customgroups/1 name=CN=
spSuperCust,OU=Groups,DC=sales,DC=oracle,DC=com

Set 'name' to 'CN=spSuperCust,OU=Groups,DC=sales,DC=oracle,DC=com'

-> set /SP/clients/ldapssl/customgroups/1 roles=au

Set 'roles' to 'au'
```

- **To view and modify information in the `userdomains` target:**

```
-> show /SP/clients/ldapssl/userdomains/1
```

For example:

```
 -> show /SP/clients/ldapssl/userdomains/1
    Targets:

    Properties:
        domain = uid=<USERNAME>,ou=people,dc=oracle,dc=com

    Commands:
        cd
        set
        show
```

Then use the `set` command to modify properties.

For example:

```
-> set SP/clients/ldapssl/userdomains1 domain=uid=<USERNAME>,
ou=people,dc=oracle,dc=oracle
```

Note – In the example above, `<USERNAME>` will be replaced with the user's login name during authentication. Names can take the form of Fully Qualified Distinguished Name (FQDN).

- **To view and modify information in the** `alternateservers` **target:**

```
-> show /SP/clients/ldapssl/alternateservers/1
```

For example:

```
-> show /SP/clients/ldapssl/alternateservers/1

/SP/clients/ldapssl/alternateservers/1
    Targets:
        cert

    Properties:
        address = 10.8.168.99
        port = 0
```

Note – In the example above, `address` can either be the IP address or DNS name. If using DNS, DNS must be enabled. For more information on enabling DNS, see ”View and Configure DNS Settings” on page 42.

Then use the `set` command to modify properties.

For example:

```
-> set /SP/clients/ldapssl/alternateservers/1 port=636
```

You can also use the `show` command to view the alternate server certificate information.

For example:

```
-> show /SP/clients/ldapssl/alternateservers/1/cert

 /SP/clients/ldapssl/alternateservers/1/cert
    Targets:

Properties:
        certstatus = certificate present
        clear_action = (none)
issuer = /C=US/O=Entrust PKI Demonstration Cerificates
        load_uri = (none)
        serial_number = 08:f23:2e:c0:8c:12:cd:bb:4e:7e:82:23:c4:0d:22:60
        subject = /C=US/O=Entrust PKI Demonstration Cerificates/OU=Entrust/Web
Connector/OU=No Liability as per http://freecerts.entrust
        valid_from = Oct 25 22:18:26 2006 GMT
        valid_until = Oct 25 22:18:26 2011 GMT
        version = 3 (0x02)
```

Type the following to copy a certificate for an alternate server:

-> set load_uri=
*<tftp|ftp|scp>***:[***<username:password>***]@//***<ipAddress|HostName>***/***<filepPath>***/**
<fileName>

The following is an example of a certificate copied using tftp:

```
-> set load_uri=tftp://10.8.172.152/sales/cert.cert
Set 'load_uri' to 'tftp://10.8.172.152/sales/cert.cert'
```

Note – The TFTP transfer method does not require a user name and password.

The following is an example of a certificate copied using tftp:

```
-> set load_uri=
ftp://sales:XpasswordX@129.148.185.50/8275_put/cert.cert
Set ’load_uri’ to
’ftp://sales:XpasswordX@129.148.185.50/8275_put/cert.cert’
```

The following is an example of a certificate copied using scp:

```
-> set
load_uri
scp://sales:XpasswordX@129.148.185.50/home/dc150698/8275_put/cert.cert
```

Type the following to remove a certificate for an alternate server:

`->` **`set clear_action=true`**

For example:

```
-> set clear_action=true
Are you sure you want to clear /SP/clients/ldapssl/cert (y/n)? y
Set ’clear_action’ to ’true’
```

- **To view and modify information in the** `optionalUserMapping` **target:**

-> show /SP/clients/ldapssl/optionalUserMapping

For example:

```
-> show

 /SP/clients/ldapssl/optionalUserMapping
    Targets:

    Properties:
        attributeInfo = (&(objectclass=person)(uid=<USERNAME>))
        binddn = cn=Manager,dc=oracle,dc=com
        bindpw = (none)
        searchbase = ou=people,dc=oracle,dc=com
        state = disabled

    Commands:
        cd
        set
         show
```

Then use the `set` command to modify properties.

For example:

```
-> set state=enabled
Set 'state' to 'enabled'
```

▼ Troubleshoot LDAP/SSL Authentication and Authorization

1. **Log in to the ILOM SP CLI or the CMM CLI.**

2. **Type the following commands:**

```
-> cd /SP/clients/ldapssl
/SP/clients/ldapssl

-> set logdetail=trace
Set 'logdetail' to 'trace'
```

3. **Perform another authorization attempt by logging out, then logging back in to the ILOM CLI and typing the following:**

```
-> show /SP/logs/event/list Class==(ldapssl) Type==(Log) Severity=
=(Trace)
```

For example:

```
-> show /SP/logs/event/list Class==(ldapssl) Type==(Log)

ID     Date/Time                  Class     Type      Severity
-----  ------------------------   --------  --------  --------
3155   Thu Nov 13 06:21:00 2008   LdapSsl   Log       critical
       (LdapSSL)  authentication status: auth-ERROR
3154   Thu Nov 13 06:21:00 2008   LdapSsl   Log       major
      (LdapSSL)  server-authenticate: auth-error idx 0 cfg-server
10.8.xxx.xxx
3153   Thu Nov 13 06:21:00 2008   LdapSsl   Log       major
       (LdapSSL)  ServerUserAuth - Error 0, error binding user to
ActiveDirectory server
```

For more information about configuring event log detail, see "View and Clear the ILOM Event Log" on page 106.

Configuring RADIUS

Topics

Description	**Links**	**Platform Feature Support**
Configure RADIUS settings	• "Configure RADIUS" on page 92	• x86 system server SP • SPARC system server SP • CMM

Before You Begin

- To configure RADIUS settings, you need the User Management (u) role enabled.

▼ Configure RADIUS

Note – If you need to provide ILOM access beyond the 10 local user accounts, and after the RADIUS server has been properly configured, you can configure ILOM to use RADIUS authentication.

---

1. **Collect the appropriate information about your RADIUS environment.**
2. **Log in to the ILOM SP CLI or the CMM CLI and use the** `cd` **command to navigate to** `/SP/clients/radius`**.**

   For example, type:

   ```
   cd  /SP/clients/radius
   ```

3. **Use the** `show` **command to view the radius properties.**

   For example, type:

   ```
   ->  show  /SP/clients/radius
   ```

```
 -> show /SP/clients/radius

   /SP/clients/radius
    Targets:

Properties:
        defaultrole = Operator
        address = 129.144.36.142
        port = 1812
        secret = (none)
        state = enabled
Commands:
        cd
        set
        show
```

4. **Use the** `set` **command to configure the radius properties described in** TABLE 4-1**.**

   `Syntax:`

   `set /SP/clients/radius [defaultrole=`
   `[Administrator|Operator|a|u|c|r|s] address=`*radius_server_IPaddress*
   `port=`*port#* `secret=`*radius_secret* `state=[`*enabled*|*disabled*`]]`

   Example:

```
 -> set /SP/clients/radius state=enabled address=10.8.145.77
Set 'state' to 'enabled'
Set 'address' to '10.8.145.77
```

TABLE 4-1 Description of Radius Properties

Property (CLI)	Default	Description
`state`	Disabled	Enabled | Disabled Specifies whether the RADIUS client is enabled or disabled.
`defaultrole` `a|u|c|r|s|Administrator|Operator`	Operator	Administrator | Operator | Advanced Roles Access role granted to all authenticated RADIUS users. This property supports the legacy roles of Administrator or Operator, or any of the individual role ID combinations of ’`a`’, ’`u`’, ’`c`’, ’`r`’, ’`o`’ and ’`s`’. For example, `aucros`, where `a`=Admin, `u`=User Management, `c`=Console, `r`=Reset and Host Control, and `s`=Service.
`ipaddress`	0.0.0.0	IP address or DNS name of the RADIUS server. If the DNS name is used, DNS must be configured and functional.
`port`	1812	Specifies the port number used to communicate with the RADIUS server. The default port is 1812.
`secret`	(none)	Specifies the shared secret that is used to protect sensitive data and to ensure that the client and server recognize each other.

CHAPTER 5

Managing System Components

Topics

Description	Links
Manage system components	• "View Component Information" on page 96 • "Prepare to Remove a Component" on page 97 • "Return a Component to Service" on page 98 • "Enable and Disable Components" on page 98

Related Topics

For ILOM	Chapter or Section	Guide
• Concepts	• About Fault Management	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide* (820-6410)
• Web interface	• Managing System Components	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* (820-6411)
• IPMI and SNMP hosts	• Inventory and Component Management	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide* (820-6413)
The ILOM 3.0 Documentation Collection is available at: `http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic`.		

Note – Syntax examples in this chapter use the target starting with `/SP/`, which could be interchanged with the target starting with `/CMM/` depending on your server platform. Subtargets are common across all Oracle Sun server platforms.

Viewing Component Information and Managing System Components

Topics

Description	Links	Platform Feature Support
Manage system components	• ”Prepare to Remove a Component” on page 97 • ”Return a Component to Service” on page 98 • ”Enable and Disable Components” on page 98	• x86 systems server SP • SPARC system server SP • CMM

Before You Begin

- To manage system components, you need the Reset and Host Control (`r`) role enabled.

View Component Information

Follow these steps to view component information:

1. **Log in to the ILOM SP CLI or the CMM CLI.**

2. **At the prompt, type:**

   ```
   -> show component_name type
   ```

   For example:

```
-> show /SYS/MB type
    Properties:
        type = Motherboard
    Commands:
        show
```

The properties that display inventory information are listed below. The properties that you are able to view depend on the target type you use.

- `fru_part_number`

- `fru_manufacturer`
- `fru_serial_number`
- `fru_name`
- `fru_description`
- `fru_version`
- `chassis_serial_number`
- `chassis_part_number`
- `product_name`
- `product_serial_number`
- `product_part_number`
- `customer_frudata`

▼ Prepare to Remove a Component

Follow these steps to prepare a component for removal:

1. **Log in to the ILOM SP CLI or the CMM CLI.**

2. **At the ILOM command prompt, type:**

   -> set *target* **prepare_to_remove_action=true**

   For example:

   ```
   -> set /CH/RFM0 prepare_to_remove_action=true
      Set 'prepare_to_remove_action' to 'true'
   ```

   After you prepare the component for removal, you can verify that it is ready to be physically removed.

3. **At the ILOM command prompt, type:**

```
—> show target prepare_to_remove_status
```

For example:

```
-> show /CH/RFM0 prepare_to_remove_status
    Properties:
        prepare_to_remove_status = Ready|NotReady
    Commands:
        cd
        set
        show
        start
        stop
```

The `Ready|NotReady` statement in the example shows whether the device is ready to be removed.

Return a Component to Service

Follow these steps to return a component to service:

Note – If you have already prepared a component for removal, and you wish to undo the action, you can do so remotely.

---

1. **Log in to the ILOM SP CLI or the CMM CLI.**

2. **At the ILOM command prompt, type:**

```
—> set target return_to_service_action=true
```

For example:

```
-> set /CH/RFM0 return_to_service_action=true
Set 'return_to_service_action' to 'true'
```

Enable and Disable Components

Follow these steps to enable and disable components:

1. **Log in to the ILOM SP CLI or the CMM CLI.**

2. **At the ILOM command prompt, type:**

```
–> set <target> component_state=enabled|disabled
```

For example:

```
-> set /SYS/MB/CMP0/P0/C0 component_state=enabled
Set ‘component_state’ to ‘enabled’
```

CHAPTER 6

Monitoring System Components

Topics

Description	Links
View and configure LEDs and system indicators	• ”View Sensor Readings” on page 102 • ”Configure System Indicators” on page 104
Set the clock and timezone	• ”Configure Clock Settings” on page 105
Filter, view, and clear event logs	• ”Filter Event Log Output” on page 106 • ”View and Clear the ILOM Event Log” on page 106
Set remote syslog receiver IP address	• ”Configure Remote Syslog Receiver IP Addresses” on page 109
View or clear faults	• ”View and Clear Faults Using the CLI” on page 110
View the SP Console History Log	• ”View and Manage SP Console History Log Entries Using the ILOM CLI” on page 111

Related Topics

For ILOM	Chapter or Section	Guide
• Concepts	• System Monitoring and Alert Management	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide* (820-6410)
• Web interface	• Monitoring System Sensors, Indicators, and ILOM Event Log	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* (820-6411)
• IPMI and SNMP hosts	• Inventory and Component Management	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide* (820-6413)

The ILOM 3.0 Documentation Collection is available at: `http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic`.

Monitoring System Sensors, Indicators, and ILOM Event Logs

Topics

Description	Links	Platform Feature Support
View and configure LEDs and system indicators	• ”View Sensor Readings” on page 102 • ”Configure System Indicators” on page 104	• x86 system server SP • SPARC system server SP • CMM
Set the clock and timezone	• ”Configure Clock Settings” on page 105	
Filter, view, and clear event logs	• ”Filter Event Log Output” on page 106 • ”View and Clear the ILOM Event Log” on page 106 • ”Configure Remote Syslog Receiver IP Addresses” on page 109	
View fault status	• ”View and Clear Faults Using the CLI” on page 110	• Most x86 system server SP • Most SPARC system server SP • CMM

▼ View Sensor Readings

Follow these steps to view sensor readings:

1. **Log in to the ILOM SP CLI or the CMM CLI.**

2. **Type the following commands to navigate to the sensor target and then to view the sensor properties:**

   ```
   ->cd target
   ->show
   ```

   For example, on some server platforms, you can specify the following path to view a temperature reading of a server's ambient air intake:

   ```
   ->cd /SYS/T_AMB
   ->show
   ```

   The properties describing the sensor target appear. For example:

```
 type = Temperature
        class = Threshold Sensor
        value = 27.000 degree C
        upper_nonrecov_threshold = 45.00 degree C
        upper_critical_threshold = 40.00 degree C
        upper_noncritical_threshold = 35.00 degree C
        lower_noncritical_threshold = 10.00 degree C
        lower_critical_threshold = 4.00 degree C
        lower_nonrecov_threshold = 0.00 degree C
        alarm_status = cleared
```

   For specific details about the type of threshold sensor targets you can access, as well as the paths to access them, consult the user documentation provided with the Sun server platform.

3. **To view a discrete sensor reading, type the following commands:**

   ```
   ->cd target
   ->show
   ```

   For example, on some Sun server platforms, you can determine whether a hard disk drive is present in slot 0 by specifying the following path:

   ```
   ->cd /SYS/HDD0_PRSNT
   ->show
   ```

   The properties describing the discrete sensor target appear. For example:

   - `Type = Entity Presence`
   - `Class = Discrete Indicator`
   - `Value = Present`

   For specific details about the type of discrete sensor targets you can access, as well as the paths to access them, consult the user documentation provided with the Sun server platform.

▼ Configure System Indicators

Before You Begin

- To configure system indicators, you need the User Management (u) role enabled.

Follow these steps to configure system indicators:

1. **Log in to the ILOM SP CLI or the CMM CLI.**

2. **To determine whether you can change the state of a system indicator, type the following commands:**

   ->cd /SYS or **cd /CH**

   ->**show**

   Targets, properties, and commands associated with the system indicator appear.

   For example:

```
 /SYS
    Targets:
        BIOS
        OK2RM
        SERVICE


    Properties:
        type = Host System
        chassis_name = SUN BLADE 8000 CHASSIS
        chassis_part_number = 602-3235-00
        chassis_serial_number = 00:03:BA:CD:59:6F
        chassis_manufacturer = SUN MICROSYSTEMS
        fault_state = OK
        clear_fault_action = (none)
        power_state = Off

    Commands:
        cd
        reset
        set
        show
        start
        stop
```

   If the set command appears in the Commands list, you can modify the state of the system indicator.

3. **To modify the state of the system indictor, type the following command:**

```
->set property=state_name
```

For more information about which system indicators are supported on your system, and the paths for accessing them, consult the user documentation provided with the Sun server platform.

▼ Configure Clock Settings

Before You Begin

- To view and set clock settings, you need the Admin (a) role enabled.

Follow these steps to configure clock settings:

1. **Log in to the ILOM SP CLI or the CMM CLI.**

2. **To view ILOM clock settings, type:**

   ```
   ->show /SP/clock
   ```

3. **To manually set the ILOM clock settings, type:**

   ```
   -> set target property_name=value
   ```

   For example:

   ```
   -> set /SP/clock datetime=MMDDhhmmYYYY
   ```

4. **To configure the ILOM clock settings to synchronize with other systems on your network by setting an IP address of an NTP server:**

   a. **To set the IP address of an NTP server, type the following command.**

   ```
   ->set /SP/clients/ntp/server/1 address=ip_address
   ```

   b. **To enable NTP synchronization, type:**

   ```
   ->set /SP/clock usentpserver=enabled
   ```

   Consult your Sun server platform user documentation for platform-specific clock information about whether:

   - The current time in ILOM persists across reboots of the SP.
   - The current time in ILOM can be synchronized with the host at host boot time.
   - There is a real-time clock element that stores the time.

▼ Filter Event Log Output

Follow these steps to filter event log output:

1. **Log in to the ILOM SP CLI or the CMM CLI.**
2. **At the command prompt, type the following:**

   ```
   -> show /SP/logs/event/list Class==(value) Type==(value)
   Severity==(value)
   ```

▼ View and Clear the ILOM Event Log

Before You Begin

- To view or clear the event log, you need the Admin (a) role enabled.

Follow these steps to view and clear the ILOM event log:

1. **Establish a local serial console connection or SSH connection to the server SP or CMM.**
2. **Type one of the following commands to set the working directory:**
   - For a rackmounted server SP: **`cd /SP/logs/event`**
   - For a blade server SP in chassis: **`cd /CH/BLn/SP/logs/event`**
   - For a CMM: **`cd /CMM/logs/event`**

3. **Type the following command to display the event log list:**

   `->`**`show list`**

   The contents of the event log appear.

   For example:

```
ID     Date/Time                 Class     Type      Severity
-----  ------------------------  --------  --------  --------
578    Wed Jun 11 06:39:47 2008  Audit     Log       minor
      user1 : Open Session : object = /session/type : value = shell
: success
577    Wed Jun 11 06:34:53 2008  Audit     Log       minor
       user1 : Set : object =
/clients/activedirectory/userdomains/3/domain : value =
<USERNAME>@joe.customer.example.sun.com : success
576    Wed Jun 11 06:25:06 2008  Audit     Log       minor
      user1 : Open Session : object = /session/type : value = www
: success
575    Wed Jun 11 06:07:29 2008  Audit     Log       minor
      user1 : Close Session : object = /session/type : value = www
: success
574    Wed Jun 11 06:02:01 2008  Audit     Log       minor
       root : Set : object =
/clients/activedirectory/dnslocatorqueries/2/service : value =
_ldap._tcp.pc._msdcs.<DOMAIN>.<PORT:636> : success
573    Wed Jun 11 06:01:50 2008  Fault     Fault     critical
     Fault detected at time = Wed Jun 11 06:01:41 2008. The suspect
component:/CH/PS3/EXTERNAL/AC_INPUT has fault.powersupply.no_ac
with probability=100 Please consult the Sun Blade 8000 Fault
Diagnosis Document (Document ID: 85878) at http://sunsolve.sun.com
to determine the correct course of action.
```

4. **In the event log, perform any of the following tasks:**
   - **Scroll down the list to view entries** – Press any key except ‘q’. The following table provides descriptions about each column appearing in the log.

Column Label	Description
Event ID	The number of the event, in sequence from number 1.
Class/Type	• Audit/ Log – Commands that result in a configuration change. Description includes user, command, command parameters, and success/fail. • IPMI/Log – Any event that is placed in the IPMI SEL is also put in the management log. • Chassis/State – For changes to the inventory and general system state. • Chassis/Action – Category for shutdown events for server module/chassis, hot insert/removal of a FRU component, and Reset Parameters button pushed. • Fault/Fault – For Fault Management faults. Description gives the time fault was detected and suspect component. • Fault/Repair – For Fault Management repairs. Description gives component.
Severity	Debug, Down, Critical, Major, or Minor
Date/Time	The day and time the event occurred. If the Network Time Protocol (NTP) server is enabled to set the ILOM time, the ILOM clock will use Universal Coordinated Time (UTC).
Description	A description of the event.

5. **To dismiss the event log (stop displaying the log), press the ‘q’ key.**

6. **To clear entries in the event log, perform the following steps:**

   a. **Type: `set clear=true`**

   A confirmation message appears.

   b. **Type one of the following:**
   - To clear the entries, type: **`y`**.
   - To cancel clearing the log, type: **`n`**.

Note – The ILOM event log accumulates many types of events, including copies of IPMI entries. Clearing the ILOM event log will clear all entries in the log, including the IPMI entries. However, clearing the ILOM event log entries will not clear the actual entries posted directly to an IPMI log.

▼ Configure Remote Syslog Receiver IP Addresses

Before You Begin

- To configure remote syslog receiver IP addresses, you need the Admin (a) role enabled.

Follow these steps to configure remote syslog receiver IP addresses:

1. **Establish a local serial console connection or SSH connection to the server SP or CMM.**

2. **Type one of the following commands to set the working directory:**

   - For a rackmounted server SP: **`cd /SP/clients/syslog`**
   - For a blade server SP in chassis: **`cd /CH/BL`*`n`*`/SP/clients/syslog`**
   - For a CMM: **`cd /CMM/clients/syslog`**

3. **Type the `show` command to display the syslog properties.**

   The properties appear. For example, accessing the syslog properties for the first time on an SP would appear as follows:

```
/SP/clients/syslog/1
Targets:
Properties:
   address = 0.0.0.0

Commands:
   cd
   set
   show
```

4. **Use the `set` command to identify a destination IP address for IP 1 (and, if applicable, IP 2).**

   For example, to set an IP destination to IP address 111.222.33.4, you would type:

   `->`**`set destination_ip1=111.222.33.4`**

5. **Press Enter for the setting to take effect.**

   The results of setting the IP address appear. For example, if you set the destination IP address to 111.222.33.4, the following would appear:

   `Set ‘destination_ip1’ to ‘111.222.33.4’`

▼ View and Clear Faults Using the CLI

Before You Begin

- To clear faults in ILOM, the Admin (a) role must be enabled and the server SP or CMM must have ILOM firmware 3.0.3 or later installed.

Follow these steps to view and clear faults using the ILOM CLI.

1. **Log in to the ILOM SP CLI or the CMM CLI.**

2. **To view a list of components that have been faulted, type:**
   - From a server:
     `->show /SP/faultmgmt`
   - From the CMM:
     `->show /CMM/faultmgmt`

3. **To display fault messages in the ILOM event log, type:**
   - From the server:
     `->show /SP/logs/event/list`
   - From the CMM:
     `->show /CMM/logs/event/list`

4. **Fix or replace the faulted component.**

5. **To clear a fault on a component, type the following command:**

```
->set component_path clear_fault_action=true
Are you sure you want to clear component_path (y/n)?  y
Set 'clear_fault_action' to 'true'
```

Where *component_path* is one of the following faulted components:

- Processor
- Memory
- Motherboard
- Fan Module
- Power Supply
- CMM
- NEM
- PCI card

For example, to clear a processor fault, you would type the following:

```
->set /SYS/MB/P0 clear_fault_action=true
Are you sure you want to clear /SYS/MB/P0 (y/n)?  y
Set 'clear_fault_action' to 'true'
```

Viewing the SP Console History Log

Topics

Description	Links	Platform Feature Support
Review the prerequisites	• "Before You Begin" on page 111	• x86 system server SP • SPARC system server SP
View the SP Console History Log	• "View and Manage SP Console History Log Entries Using the ILOM CLI" on page 111	

Note – The SP Console History Log feature is not available for use from the ILOM web interface.

For instructions about how to display log entries in the SP Console History Log file, see the following procedure.

Before You Begin

- You must have Console (c) role user account to display the entries stored in the SP Console History Log file.
- You must be using ILOM 3.0.8 or a later version of ILOM to view the SP Console History Log on Oracle x86 servers. Prior to ILOM 3.0.8, the SP Console History Log file was only viewable in ILOM on Oracle SPARC servers.

▼ View and Manage SP Console History Log Entries Using the ILOM CLI

1. **Log in to the ILOM SP CLI.**

2. **Use the** `show` **command to display the SP Console target, properties, and commands.**

   For example:

```
-> show /SP/console

 /SP/console
    Targets:
        history

    Properties:
        line_count = 0
        pause_count = 0
        start_from = end

    Commands:
        cd
        show
        start
        stop
->
```

3. **Use the** `help` **command to view details about the SP Console target and properties.**

   For example:

```
-> help /SP/console

 /SP/console: Redirection of console stream to SP
    Targets:
        history: console history

    Properties:
        line_count: total number of lines to display
       line_count: Possible values = 0-2048 where 0 means no limit
        line_count: User role required for set = c

        pause_count: number of lines to display before each pause
      pause_count: Possible values = 0-2048 where 0 means no limit
        pause_count: User role required for set = c

       start_from: from which end of the available history to list
        start_from: Possible values = beginning,end
        start_from: User role required for set = c

```

4. **Use the** `set` **command to specify the property values that you want ILOM to use when displaying the entries in the SP Console History Log file**.

   For example:

   - `set` command usage:

     `set [target] <property>=<value> [<property>=<value>...]`

   - At the prompt, you would type the SP console target and one or more display property values as follows:

     -> **`set /SP/console`** *property*=*value*

     -> **`set /SP/console`** *property*=*value* *property*=*value*

     -> **`set /SP/console`** *property*=*value* *property*=*value* *property*=*value*

   Where *property* and *value* can be any of the following parameters specified in the following table.

Property	Values	Example
`line_count`	Accepts a line value within the range of `0` to `2048`, where `0` means no limit. **Note -** The default value for `line_count` is `0`.	To specify ILOM to display four lines of the SP Console History Log, you would type: **`-> set /SP/console line_count=4`**
`pause_count`	Accepts a pause value within the range of `0` to `2048`, where `0` means not to pause the display. **Note -** The default value for `pause_count` is `0`.	To specify ILOM to display four lines of the SP Console History Log and pause the display after displaying two lines, you would type: -> **`set /SP/console line_count=4 pause_count=2`**
`start_from`	Values include: • `end` – The last line (most recent) in the history log. • `beginning` - The first line in the history log. **Note -** The default value for `start_from` is `end`.	To specify ILOM to display the first four lines of the SP Console History Log and pause the display after displaying two lines, you would type: -> **`set /SP/console line_count=4 pause_count=2 start_from=beginning`**

The UTC timestamps recorded in the SP Console History Log reflect the local time configured on the server.

CHAPTER 7

Monitoring Storage Components and Zone Manager

Topics

Description	Links
View and monitor storage details for HDDs and RAID controllers	• ”Show Property Details for HDDs and RAID Controllers” on page 117
Enable or disable Zone Manager	• “Enabling or Disabling Zone Manager” on page 120

Related Topics

For ILOM	Chapter or Section	Guide
• Concepts	• Storage Monitoring and Zone Management	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide* (820-6410)
• Web interface	• Monitoring Storage Components and Zone Manager	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* (820-6411)

The ILOM 3.0 Documentation Collection is available at: `http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic`.

Viewing and Monitoring Storage Components

Topics

Description	Links	Platform Feature Support
Review the prerequisites	• "Before You Begin" on page 116	• x86 system server SP
Show property details for HDDs and RAID controllers	• "Show Property Details for HDDs and RAID Controllers" on page 117	

Before You Begin

- Ensure that the Storage Monitoring feature is supported on your Sun server. For details, see the ILOM Supplement guide or platform Administration guide for your server.
- You must be using ILOM 3.0.6 or a later version of ILOM.
- For Sun servers supporting the Storage Monitoring features, you must download and install a system management pack prior to using the Storage Monitoring features in ILOM. For information about how to download this management pack, see *Oracle Server Hardware Management Pack User's Guide* (821-1609).
- Some Sun servers might not enable support for the storage monitoring functions that are described in this chapter. To determine whether storage monitoring support on your server has been enabled, see the ILOM Supplement guide or platform Administration guide for your server.
- For Sun servers supporting the Storage Monitoring feature in ILOM, a system management pack must be installed to use the Storage Monitoring features. For information about how to download this management pack, see *Oracle Server Hardware Management Pack User's Guide* (821-1609).
- For conceptual information and examples on viewing and monitoring storage components, see the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide* (820-6410).

▼ Show Property Details for HDDs and RAID Controllers

1. **Log in to the ILOM SP CLI.**

Note – Alternatively, you can log in to the ILOM CMM CLI then navigate to the SP target where you can display the HDD details under `/SYS` or the RAID disk controller details under `/STORAGE/raid`.

---

2. **Use the `cd` command to navigate to the `/SYS` or `/STORAGE/raid` target.**

   For example:

   - `->`**`cd /SYS`**

   or

   - `->`**`cd /STORAGE/raid`**

3. **To display property details for an HDD installed on your server, use the `show` command.**

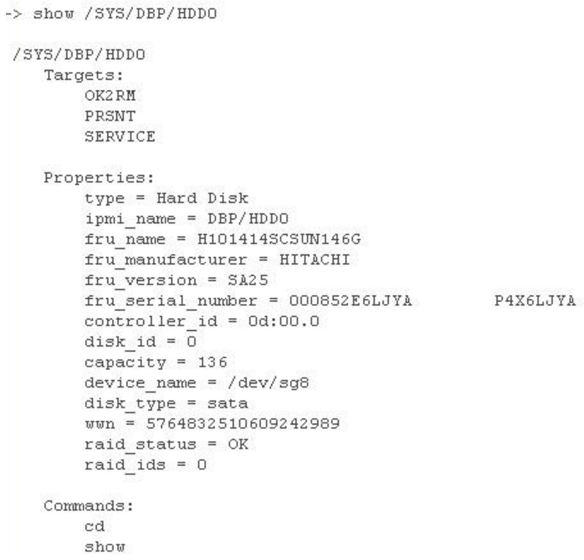
   For example:

   - To view storage details for a specific HDD configured on your system, you might type:

     `->` **`show /SYS/DBP/HDD`***0*

Where *0* is the HDD slot location on the server where the HDD is installed.

Sample CLI output:



```
-> show /SYS/DBP/HDD0

 /SYS/DBP/HDD0
    Targets:
        OK2RM
        PRSNT
        SERVICE

    Properties:
        type = Hard Disk
        ipmi_name = DBP/HDD0
        fru_name = H101414SCSUN146G
        fru_manufacturer = HITACHI
        fru_version = SA25
        fru_serial_number = 000852E6LJYA        P4X6LJYA
        controller_id = 0d:00.0
        disk_id = 0
        capacity = 136
        device_name = /dev/sg8
        disk_type = sata
        wwn = 5764832510609242989
        raid_status = OK
        raid_ids = 0

    Commands:
        cd
        show
```

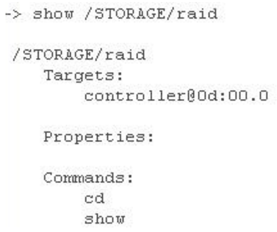
4. **To display property details associated with a RAID controller and its associated disk IDs, use the** `show` **command:**

   For example:

   a. **To list the RAID controller target(s) configured, you would type:**

   -> **`show /STORAGE/raid`**

   Sample CLI storage raid target output:



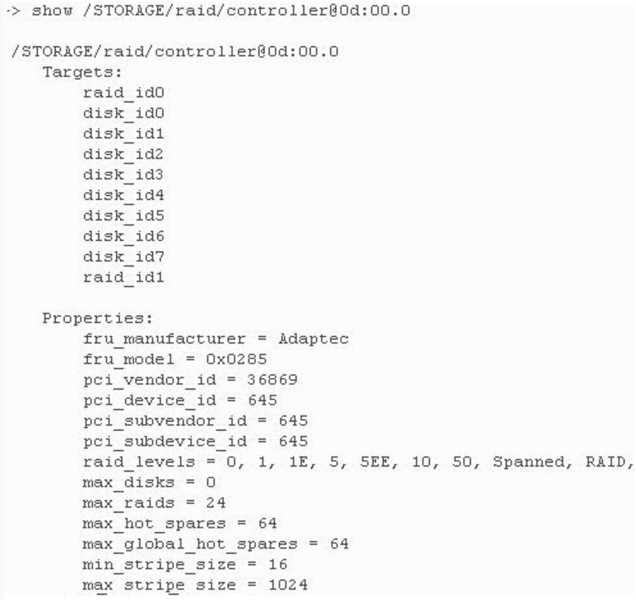
```
-> show /STORAGE/raid

 /STORAGE/raid
    Targets:
        controller@0d:00.0

    Properties:

    Commands:
        cd
        show
```

   b. **To show the property details associated with a controller, as well as to list the raid_id targets configured, you would type:**

   -> **`show /STORAGE/raid/controller@od:`***00.0*

   Where `od:`*00.0* is the ID that corresponds to the PCI address of the controller.

   Sample CLI RAID controller targets and properties output:



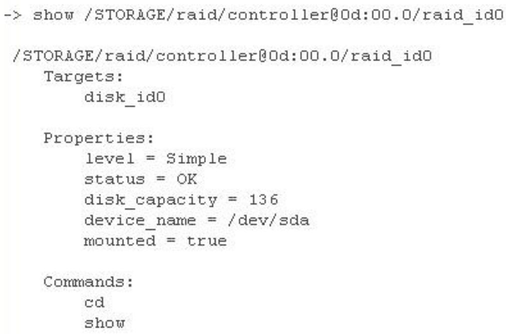
```
-> show /STORAGE/raid/controller@0d:00.0

 /STORAGE/raid/controller@0d:00.0
    Targets:
        raid_id0
        disk_id0
        disk_id1
        disk_id2
        disk_id3
        disk_id4
        disk_id5
        disk_id6
        disk_id7
        raid_id1

    Properties:
        fru_manufacturer = Adaptec
        fru_model = 0x0285
        pci_vendor_id = 36869
        pci_device_id = 645
        pci_subvendor_id = 645
        pci_subdevice_id = 645
        raid_levels = 0, 1, 1E, 5, 5EE, 10, 50, Spanned, RAID,
        max_disks = 0
        max_raids = 24
        max_hot_spares = 64
        max_global_hot_spares = 64
        min_stripe_size = 16
        max_stripe_size = 1024
```

c. **To list the available disk_id targets, as well as to view the properties associated with a controller raid_id, you would type:**

-> **show /STORAGE/raid/controller@od:***00.0***/raid_id***0*

- Where od:*00.0* is the PCI address for the controller that was found installed on your server.
- Where raid_id*0* is the target RAID disk that is configured on the controller.

Sample CLI RAID controller output for raid_id:



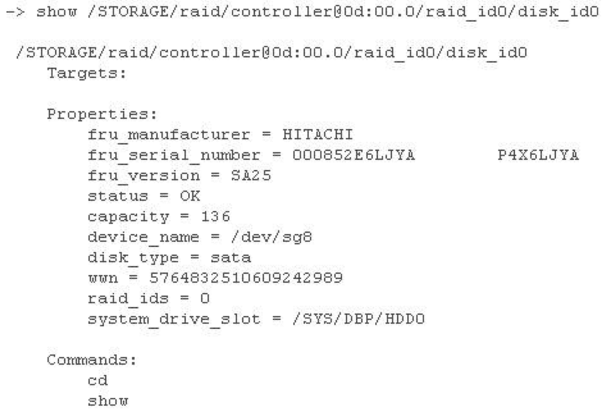
```
-> show /STORAGE/raid/controller@0d:00.0/raid_id0

 /STORAGE/raid/controller@0d:00.0/raid_id0
    Targets:
        disk_id0

    Properties:
        level = Simple
        status = OK
        disk_capacity = 136
        device_name = /dev/sda
        mounted = true

    Commands:
        cd
        show
```

d. **To view the property details for a disk_id that is associated with a raid_id on the controller, you would type:**

-> **show /STORAGE/raid/controller@od:***00.0***/raid_id***0***/disk_id***0*

- Where `od:`*00.0* is the PCI address for the controller that was found installed on your server.
- Where `raid_id`*0* is the target RAID disk that is configured on the controller.
- Where `disk_id`*0* is the target disk that is associated with the raid_id.

Sample CLI RAID controller output for raid_id and disk_id:



```
-> show /STORAGE/raid/controller@0d:00.0/raid_id0/disk_id0

 /STORAGE/raid/controller@0d:00.0/raid_id0/disk_id0
    Targets:

    Properties:
        fru_manufacturer = HITACHI
        fru_serial_number = 000852E6LJYA        P4X6LJYA
        fru_version = SA25
        status = OK
        capacity = 136
        device_name = /dev/sg8
        disk_type = sata
        wwn = 5764832510609242989
        raid_ids = 0
        system_drive_slot = /SYS/DBP/HDD0

    Commands:
        cd
        show
```

5. **Type `exit` to exit the CLI.**

Enabling or Disabling Zone Manager

If you are using Oracle Sun Blade 6000 or Sun Blade 6048 Modular Systems, a new zone management feature was added as of ILOM 3.0.10. The zone management feature is available for SAS-2 storage devices that are installed in Oracle Sun Blade 6000 or Sun Blade 6048 Modular Systems. For more information about how to manage SAS-2 chassis storage devices from ILOM, see the *Oracle Integrated Lights Out Manager (ILOM) CMM Administration Guide for Sun Blade 6000 and Sun Blade 6048 Modular Systems* (820-0052).

CHAPTER 8

Managing System Alerts

Topics

Description	Links
Review the prerequisites	• "Before You Begin" on page 122
Manage alert rule configurations	• "Create or Edit Alert Rules" on page 123 • "Disable an Alert Rule" on page 124
Generate test alerts to confirm alert configuration is working	• "Generate Test Alerts" on page 124
Send a test email alert before saving an alert rule	• "Send Test Email Alert to a Specific Destination" on page 124
Review the CLI commands you need to use when managing alert rule configurations	• "CLI Commands for Managing Alert Rule Configurations" on page 125
Notify recipient of system alerts using email	• "Enable SMTP Client" on page 127
Download SNMP MIBs directly from ILOM	• "Download SNMP MIBs" on page 129

Related Topics

For ILOM	Chapter or Section	Guide
• Concepts	• System Monitoring and Alert Management	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide* (820-6410)

The ILOM 3.0 Documentation Collection is available at: http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic.

Related Topics

For ILOM	Chapter or Section	Guide
• Web interface	• Managing System Alerts	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* (820-6411)
• IPMI and SNMP hosts	• Inventory and Component Management	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide* (820-6413)

The ILOM 3.0 Documentation Collection is available at:
`http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic`.

Managing Alert Rule Configurations

Topics

Description	Links	Platform Feature Support
Review the prerequisites	• "Before You Begin" on page 122	• x86 system server SP • SPARC system server SP • CMM
Configure alert configurations	• "Create or Edit Alert Rules" on page 123 • "Disable an Alert Rule" on page 124	
Generate test alerts to confirm alert configuration is working	• "Generate Test Alerts" on page 124	
Send a test email alert to a specific destination before saving the alert rule	• "Send Test Email Alert to a Specific Destination" on page 124	
Notify recipient of system alerts via email	• "Enable SMTP Client" on page 127	

Before You Begin

- If you are defining an Email Notification alert, the outgoing email server that will be used to send the email notification must be configured in ILOM. If an outgoing email server is not configured, ILOM will not be able to successfully generate Email Notification alerts.

- If you are defining an SNMP Trap alert with the version set to SNMP v3, the SNMP user name must be defined in ILOM as an SNMP user. If the user is not defined in ILOM as an SNMP user, the receiver of the SNMP alert will be unable to decode the SNMP alert message.
- Review the CLI commands for managing alert rule configurations. See "CLI Commands for Managing Alert Rule Configurations" on page 125.
- To manage alert rule configurations, you need the Admin (a) role enabled.
- To send a test email alert, you need the Read Only (o) role enabled and you must be using ILOM 3.0.4 or a later version of ILOM.

▼ Create or Edit Alert Rules

Follow these steps to configure an alert rule:

1. **Establish a local serial console connection or SSH connection to the server SP or CMM.**
2. **Type one of the following command paths to set the working directory:**
   - For a rackmounted server: **`cd /SP/alertmgmt`**
   - For a blade server module: **`cd /SP/alertmgmt`**
   - For a chassis CMM: **`cd /CMM/alertmgmt`**
3. **Type the `show` command to view properties associated with an alert rule.**

   For example, to view the properties associated with the first alert rule, you would type one of the following:

   - For a rackmounted server: **`show /SP/alertmgmt/rules/1`**
   - For a blade sever module: **`show /CH/BL`*n*`/SP/alertmgmt/rules/1`**
   - For a chassis CMM: **`show /CMM/alertmgmt/CMM/rules/1`**
4. **Type the `set` command to assign values to properties associated with an alert rule.**

   For example, to set IPMI PET as the alert type for rule 1, you would type the following command path:

   ```
   ->set /SP/alertmgmt/rules/1 type=ipmipet
   ```

Note – To enable an alert rule configuration, you must specify a value for the alert type, alert level, and alert destination. If you are defining an SNMP alert type, you can optionally define a value for authenticating the receipt of SNMP Trap alerts.

▼ Disable an Alert Rule

Follow these steps to disable an alert rule:

1. **Establish a local serial console connection or SSH connection to the server SP or CMM.**
2. **Type one of the following command paths to set the working directory:**
   - For a rackmounted server SP, type: **`cd /SP/alertngnt/rules/`***n*
   - For a blade server SP, type: **`cd /CH/BL`***n***`/SP/alertmgmt/rules/`***n*
   - For a chassis CMM, type: **`cd /CMM/alertmgmt/CMM/rules/`***n*

   Where *n* equals a specific alert rule number, which can be 1 to 15.

   [BL*n* refers to the server module (blade) slot number.]
3. **To disable the alert rule, type the following command:**

```
->set level=disable
```

▼ Generate Test Alerts

Follow these steps to generate test alerts:

1. **Establish a local serial console connection or SSH connection to the server SP or CMM.**
2. **Type one of the following command paths to set the working directory:**
   - For a rackmounted server SP, type: **`cd /SP/alertmgmt/rules`**
   - For a blade server SP, type: **`cd /CH/BL`***n***`/SP/alertmgmt/rules`**
   - For a chassis CMM, type: **`cd /CMM/alertmgmt/CMM/rules`**
3. **Type the following command to generate a test alert for each enabled alert rule configuration:**

```
->set testalert=true
```

▼ Send Test Email Alert to a Specific Destination

Follow these steps to send a test email alert:

1. **Establish a local serial console connection or SSH connection to the server SP or CMM.**
2. **Type one of the following command paths to set the working directory:**

- For a rackmounted server SP, type: **`cd /SP/alertmgmt/rules`**
- For a blade server SP, type: **`cd /CH/BL`*n*`/SP/alertmgmt/rules`**
- For a chassis CMM, type: **`cd /CMM/alertmgmt/CMM/rules`**

3. **Type the following command to send a test email alert for each alert rule configuration:**

```
->set testrule=true
```

CLI Commands for Managing Alert Rule Configurations

The following table describes the CLI commands that you will need to use to manage alert rule configurations using the ILOM CLI.

TABLE 8-1 CLI Commands for Managing Alert Rule Configurations

CLI Command	Description

`show`	The `show` command enables you to display any level of the alert management command tree by specifying either the full or relative path.
	Examples:
	• To display an alert rule along with its properties using a full path, you would type the following at the command prompt:
	`-> show /SP/alertmgmt/rules/1`
	`/SP/alertmgmt/rules/1`
	`Properties:`
	`    community_or_username = public`
	`        destination = 129.148.185.52`
	`        level = minor`
	`        snmp_version = 1`
	`        type = snmptrap`
	`Commands:`
	`        cd`
	`        set`
	`        show`

TABLE 8-1 CLI Commands for Managing Alert Rule Configurations *(Continued)*

CLI Command	Description

	• To display a single property using the full path, you would type the following at the command prompt:
	`-> show /SP/alertmgmt/rules/1 type`
	`/SP/alertmgmt/rules/1`
	`Properties:`
	`type = snmptrap`
	`Commands:`
	`set`
	`show`
	• To specify a relative path if the current tree location is `/SP/alertmgmt/rules`, you would type the following at the command prompt:
	`-> show 1/`
	`/SP/alertmgmt/rules/1`
	`Targets:`
	`Properties:`
	`community_or_username = public`
	`destination = 129.148.185.52`
	`level = minor`
	`snmp_version = 1`
	`type = snmptrap`
	`Commands:`
	`cd`
	`set`
	`show`

`cd`	The `cd` command enables you to set the working directory. To set alert management as a working directory on a server SP, you would type the following command at the command prompt: **`-> cd /SP/alertmgmt`**
`set`	The `set` command enables you to set values to properties from any place in the tree. You can specify either a full or relative path for the property depending on the location of the tree. For example: • For full paths, you would type the following at the command prompt: **`-> set /SP/alertmgmt/rules/1 type=ipmipet`** • For relative path (tree location is `/SP/alertmgmt`), you would type the following command path at the command prompt: **`-> set rules/1 type=ipmipet`** • For relative path (tree location is `/SP/alertmgmt/rules/1`), you would type the following command path at the command prompt: **`-> set type=ipmipet`**

Configuring SMTP Client for Email Notification Alerts

Topics

Description	Links	Platform Feature Support
Notify recipient of system alerts using email	• "Enable SMTP Client" on page 127	• x86 system server SP • SPARC system server SP • CMM

Before You Begin

- To enable SMTP Clients, you need the Admin (a) role enabled.
- To generate configured Email Notification alerts, you must enable the ILOM client to act as an SMTP client to send the email alert messages.
- Prior to enabling the ILOM client as an SMTP client, determine the IP address and port number of the outgoing SMTP email server that will process the email notification.

▼ Enable SMTP Client

Follow these steps to enable the SMTP client:

1. **Establish a local serial console connection or SSH connection to the server SP or CMM.**
2. **Type one of the following command paths to set the working directory:**
   - For a rackmounted server SP, type: **`cd /SP/clients/smtp`**
   - For a blade server SP, type: **`cd /CH/BL`*`n`*`/SP/clients/smtp`**
   - For a chassis CMM, type: **`cd /CMM/clients/smtp`**

3. **Type the** `show` **command to display the SMTP properties.**

   For example, accessing the SMTP properties for the first time on an SP would appear as follows:

```
-> show
/SP/clients/smtp
Targets
  Properties
  address = 0. 0. 0. 0
  port = 25
  state = enabled
Commands:
  cd
  set
  show
```

4. **Use the** `set` **command to specify an IP address for the SMTP client or to change the port or state property value.**

   For example:

```
->set address=222.333.44.5
```

5. **Press Enter for the change to take effect.**

   For example, if you typed `set address=222.333.44.5` the following result would appear:

```
Set ‘address=222.333.44.5’
```

Downloading SNMP MIBs Directly From ILOM

Topics

Description	Links	Platform Feature Support
Download SNMP MIBs directly from ILOM	• "Download SNMP MIBs" on page 129	• x86 system server SP • SPARC system server SP • CMM

Before You Begin

- The Reset and Host Control (r) role is required to download SNMP MIBs from ILOM.
- You must be using ILOM 3.0.4 or a later version of ILOM.

▼ Download SNMP MIBs

Follow these steps to download SNMP MIBs:

1. **Log in to the ILOM SP CLI or the CMM CLI.**
2. **Use the** show **command to display the SNMP MIBs.**

   For example:

```
 -> show /SP/services/snmp/mibs

  /SP/services/snmp/mibs
     Targets:

     Properties:
         dump_uri = (Cannot show property)

     Commands:
         cd
         dump
         set
         show
```

3. **To download the files, type either of the following commands:**

   ```
   -> dump -destination URI /SP/services/snmp/mibs
   ```

   or

   ```
   -> set /SP/services/snmp/mibs dump_uri=URI
   ```

   Where *URI* specifies the target to which the files are downloaded.

   A zip file containing the MIBs are transferred to the destination server.

CHAPTER 9

Power Monitoring and Management of Hardware Interfaces

Topics

Description	Links
Identify power monitoring and management feature updates per ILOM firmware point release	• "Summary of Power Management Feature Updates" on page 132
CLI procedures for power monitoring and management of hardware interfaces	• "Monitoring System Power Consumption" on page 134 • "Configuring Power Policy Settings to Manage Server Power Usage" on page 142 • "Configuring Power Consumption Threshold Notifications" on page 143 • "Monitoring Component Power Allocation Distributions" on page 144 • "Configuring Power Limit Properties" on page 149 • "Monitoring or Configuring CMM Power Supply Redundancy Properties" on page 155

Related Topics

For ILOM	Chapter or Section	Guide
• Concepts	• Power Consumption Management Interfaces	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide* (820-6410)

The ILOM 3.0 Documentation Collection is available at: `http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic`.

Related Topics

For ILOM	Chapter or Section	Guide
• Web interface	• Monitoring Power Consumption	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* (820-6411*)*
• IPMI and SNMP hosts	• Monitoring Power Consumption	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide* (820-6413)
• Feature Updates	• Power Management Feature Updates	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Features Updates and Release Notes* (820-7329).

The ILOM 3.0 Documentation Collection is available at:
http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic.

Summary of Power Management Feature Updates

TABLE 9-1 identifies the common power management feature enhancements and documentation updates made since ILOM 3.0.

TABLE 9-1 Power Management Feature Updates per ILOM Firmware Point Release

New or Enhanced Feature	Firmware Point Release	Documentation Updates	For Updated CLI Procedures, see:
Monitor Power Consumption Metrics	ILOM 3.0	• New terms and definitions for Power Management Metrics • New System Monitoring --> Power Management Consumption Metric properties • New CLI and web procedures added for monitoring device power consumption	• "Monitoring System Power Consumption" on page 134
Configure Power Policy Properties	ILOM 3.0	• New power policy properties explained. • New CLI and web procedures added for configuring power policy settings	• "Configuring Power Policy Settings to Manage Server Power Usage" on page 142
Monitor Power Consumption History	ILOM 3.0.3	• New power consumption history metrics • New CLI and web procedures added for monitoring power consumption	• "Monitor Power Consumption History" on page 138

TABLE 9-1 Power Management Feature Updates per ILOM Firmware Point Release *(Continued)*

New or Enhanced Feature	Firmware Point Release	Documentation Updates	For Updated CLI Procedures, see:
Configure Power Consumption Notification Thresholds	ILOM 3.0.4	• New power consumption notification threshold settings • New CLI and web procedures added for configuring the power consumption thresholds	• "Configuring Power Consumption Threshold Notifications" on page 143
Monitor Allocation Power Distribution Metrics	ILOM 3.0.6	• New component allocation distribution metrics • New CLI and web procedures added for monitoring power allocations • New CLI and web procedures added for configuring permitted power for blade slots	• "Monitoring Component Power Allocation Distributions" on page 144
Configure Power Budget Properties	ILOM 3.0.6	• New power budget properties • New CLI and web procedures added for configuring power budget properties	• "Configuring Power Limit Properties" on page 149
Configure Power Supply Redundancy Properties for CMM Systems	ILOM 3.0.6	• New power supply redundancy properties for CMM system. • New CLI and web procedures added for configuring power supply redundancy properties on CMM systems	• "Monitoring or Configuring CMM Power Supply Redundancy Properties" on page 155
CLI Update for CMM Power Management	ILOM 3.0.10	• New top-level tab added to ILOM web interface for Power Management • Revised CLI commands for CMM • Power Management Metrics tab removed from CMM ILOM web interface • Updated CLI procedure for configuring a grant limit for blade slots (previously known as allocatable power)	• "View Blade Slots Granted Power or Reserved Power as of ILOM 3.0.10" on page 147 • "View Granted Power or Grant Limit for Blade as of ILOM 3.0.10" on page 148 • "Configure Grant Limit for aBlade as of ILOM 3.0.10" on page 154

Monitoring System Power Consumption

c

Topics

Description	Links	Platform Feature Support
Monitor power consumption	• ”Monitor Total System Power Consumption” on page 135 • ”Monitor Actual Power Consumption” on page 136 • ”Monitor Individual Power Supply Consumption” on page 136 • ”Monitor Available Power” on page 137 • ”Monitor Server Hardware Maximum Power Consumption” on page 138 • ”Monitor Permitted Power Consumption” on page 138	• x86 system server SP • SPARC system server SP • CMM
Monitor power consumption history	• ”Monitor Power Consumption History” on page 138	• x86 system server SP • SPARC system server SP • CMM

Before You Begin

- Review the Power Monitoring Terminology defined in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide.*

Note – The power consumption features described in this chapter might not be implemented on your platform server or CMM. To determine whether the power consumption features described in this section are supported on your server or CMM, see the ILOM Supplement or Administration guide provided for your server.

- To access the power consumption metrics provided by ILOM you must be running ILOM 3.0 or later. To access the power consumption history, you must be running ILOM 3.0.3 or later.

Note – Power consumption history is provided using the ILOM CLI and web interfaces. This information is not available through IPMI or SNMP.

- Some platform servers might provide additional platform-specific power metrics under the `/SP/powermgmt/advanced` node. To determine whether your system supports additional platform-specific power metrics, see the ILOM Supplement Guide or administration guide provided for your server.

▼ Monitor Total System Power Consumption

1. **Log in to the ILOM SP CLI or the ILOM CMM CLI.**

2. **Type the** `show` **command to display the total power consumption.**

   For example:

   - On the server SP, type:

     ```
     -> show /SYS/VPS
     ```

   - On the CMM, type:

     ```
     ->  show /CH/VPS
     ```

```
/CH/VPS
   Targets:
       history

   Properties:
       type = Power Unit
       ipmi_name = VPS
       class = Threshold Sensor
       value = 898.503 Watts
       upper_nonrecov_threshold = N/A
       upper_critical_threshold = N/A
       upper_noncritical_threshold = N/A
       lower_noncritical_threshold = N/A
       lower_critical_threshold = N/A
       lower_nonrecov_threshold = N/A
       alarm_status = cleared

   Commands:
       cd
       show
```

The following table lists and describes the properties of the Total Power Consumption sensor for CLI.

Property	Value
`type`	Threshold values are platform specific. Refer to your platform documentation for details.
`class`	
`value`	
`upper_nonrecov_threshold`	
`upper_critical_threshold`	
`upper_noncritical_threshold`	
`lower_noncritical_threshold`	
`lower_critical_threshold`	
`lower_nonrecov_threshold`	

▼ Monitor Actual Power Consumption

1. **Log in to the ILOM server SP CLI or ILOM CMM CLI.**
2. **Type the** `show` **command to display the actual power consumption.**

   For example:

   - For the server SP, type:

     ```
     -> show /SP/powermgmt actual_power
     ```

   - For the CMM, type:

     ```
     -> show /CMM/powermgmt actual_power
     ```

Note – The `actual_power` is the same as `/SYS/VPS`. The `actual_power` is the value returned by the sensor.

▼ Monitor Individual Power Supply Consumption

1. **Log in to the ILOM server SP CLI or ILOM CMM CLI.**
2. **Type the** `show` **command to display the individual power supply consumption.**

   For example:

   - For CLI on rackmounted system:

     ```
     -> show /SYS/platform_path_to_powersupply/INPUT_POWER|OUTPUT_POWER
     ```

- For CLI on CMM:

```
-> show /CH/platform_path_to_powersupply/INPUT_POWER|OUTPUT_POWER
```

The following table lists and describes the properties of the CLI sensors. Both sensors, INPUT_POWER and OUTPUT_POWER, have the same properties.

Property	Value
`type`	Power Unit
`class`	Threshold Sensor
`value`	<total consumed power in watts, for example "1400">
`upper_nonrecov_threshold`	N/A
`upper_critical_threshold`	N/A
`upper_noncritical_threshold`	N/A
`lower_noncritical_threshold`	N/A
`lower_critical_threshold`	N/A
`lower_nonrecov_threshold`	N/A

Note – Power sensors are not supported on server modules (blades).

▼ Monitor Available Power

1. **Log in to the ILOM server SP CLI or the ILOM CMM CLI.**
2. **Type the** `show` **command to display the available power.**

   For example:

   - For CLI on a rackmounted system:

   ```
   -> show /SP/powermgmt available_power
   ```

   - For CLI on a CMM:

   ```
   -> show /CMM/powermgmt available_power
   ```

▼ Monitor Server Hardware Maximum Power Consumption

1. **Log in to the ILOM server SP CLI.**
2. **Type the** `show` **command to display the hardware configuration maximum power consumption.**

   For example:

```
-> show /SP/powermgmt hwconfig_power
```

▼ Monitor Permitted Power Consumption

1. **Log in to the ILOM Server SP CLI or the ILOM CMM CLI.**
2. **Type the** `show` **command to display the permitted power consumption.**

   For example:

   - For CLI on a rackmounted system:

```
->  show /SP/powermgmt permitted_power
```

   - For CLI on a CMM:

```
-> show /CMM/powermgmt permitted_power
```

▼ Monitor Power Consumption History

1. **Log in to ILOM the server SP CLI or the ILOM CMM CLI.**
2. **Use the show command to view actual power consumption.**

   For example:

   - From the server SP:

```
->show /SYS/VPS
```

   - From a server module in a chassis:

```
->show /CMM/BLn/VPS
```

   - From the CMM:

```
->show /CH/VPS
```

```
->show /CH/VPS

 /CH/VPS
    Targets:
        history

    Properties:
        type = Power Unit
        ipmi_name = VPS
        class = Threshold Sensor
        value = 1400.000 Watts
        upper_nonrecov_threshold = N/A
        upper_critical_threshold = N/A
        upper_noncritical_threshold = N/A
        lower_noncritical_threshold = N/A
        lower_critical_threshold = N/A
        lower_nonrecov_threshold = N/A
        alarm_status = cleared

    Commands:
        cd
        show
```

3. **Use the** `show` **command to display 15-, 30-, and 60-second rolling power usage average, and to display a choice of targets for average consumption history.**

   For example:

   - From the server SP, type:

     `->`**`show /SYS/VPS/history`**

   - From the CMM, type:

```
->show /CH/VPS/history
```

```
->show /CH/VPS/history

 /CH/VPS/history
    Targets:
        0 (1 Minute Average, 1 Hour History)
        1 (1 Hour Average, 14 Day History)

    Properties:
        15sec_average = 1210.000
        30sec_average = 1400.000
        60sec_average = 1800.000

    Commands:
        cd
        show
```

4. **Use the** `show` **command to display average consumption history by the minute or hour respectively, type the following command with the appropriate target named.**

   For example

   - From the server SP, type:

     ```
     ->show /SYS/VPS/history/0
     ```

   - From the CMM:

     ```
     ->show /CH/VPS/history/0
     ```

   For example:

```
->show /CH/VPS/history/0

/CH/VPS/history/
   Targets:
       list

   Properties:
       average = 1500.000
       minimum = 1500.000 at Mar  4 08:51:24
       maximum = 1500.000 at Mar  4 08:51:23
       period = 1 Minute Average
       depth = 1 Hour History

   Commands:
       cd
       show
```

5. **Use the** `show` **command to display sample set details such as time stamp and power consumed in watts.**

   For example:

   - From the server SP, type:
     `->`**`show /SYS/VPS/history/0/list`**
   - From the CMM, type:
     `->`**`show /CH/VPS/history/0/list`**

```
->show /CH/VPS/history/0/list

/CH/VPS/history/0/list
   Targets:

   Properties:
       Mar  4 08:52:23 = 1500.000
       Mar  4 08:51:24 = 1500.000
       Mar  4 08:50:24 = 1500.000
       Mar  4 08:49:24 = 1500.000
       Mar  4 08:48:24 = 1500.000
       Mar  4 08:47:23 = 1500.000
    Commands:
       cd
       show
```

Configuring Power Policy Settings to Manage Server Power Usage

Topics

Description	Links	Platform Feature Support
Configure power policy	• "Configure Server SP Power Policy" on page 142	• x86 system server SP (prior to ILOM 3.0.4) • SPARC system server SP

Before You Begin

- Review the Power Monitoring Terminology defined in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide.*

Note – The power policy feature described in this section might not be implemented on the platform server or CMM that you are using. To determine whether the power consumption feature described in this section are supported on your server or CMM, see the ILOM Supplement or Administration guide provided for your server.

- To configure the Power Policy properties in ILOM for x86 servers, you must have Administrator (a) role privileges and you must be running ILOM 3.0.3 or earlier.
- To configure the Power Policy properties in ILOM for SPARC servers, you must have Administrator (a) role privileges and you must be running ILOM 3.0 or later.

▼ Configure Server SP Power Policy

1. **Log in to the ILOM server SP CLI.**
2. **Type the `set` command to set the power policy:**

```
-> set /SP/powermgmt policy=Performance|Elastic
```

3. **Type the `show` command to display the power policy:**

```
-> show /SP/powermgmt policy
```

Configuring Power Consumption Threshold Notifications

Topics

Description	Links	Platform Feature Support
View or configure power consumption notification thresholds	• ”View and Configure Notification Thresholds Using the CLI” on page 143	• x86 system server SP • SPARC system server SP • CMM

Before You Begin

- Review the Power Monitoring Terminology defined in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide.*
- You must have ILOM 3.0.4 or later installed on your server or CMM.
- You must have Administrator (a) privileges in ILOM to change power consumption configuration variables.

▼ View and Configure Notification Thresholds Using the CLI

1. **Log in to ILOM server SP CLI or the ILOM CMM CLI.**
2. **To view the current settings, type:**

   ```
   -> show /SP/powermgmt
   ```

   or

   ```
   -> show /CMM/powermgmt
   ```

3. **To set the value for notification thresholds, type:**

   ```
   -> set threshold1|2=n
   ```

   Where *n* represents watts.

Note – Setting the notification threshold value to `0` (zero) will disable the notification threshold option.

Monitoring Component Power Allocation Distributions

Topics

Description	Links	Platform Feature Support
View component allocation metrics for server or CMM	• ”View Server Power Allocations for All System Components” on page 145 • ”View Server Component Power Allocations” on page 145 • ”View CMM Power Allocations for All Chassis Components” on page 146 • ”View CMM Component Power Allocations” on page 147 • ”View Blade Slots Granted Power or Reserved Power as of ILOM 3.0.10” on page 147 • ”View Granted Power or Grant Limit for Blade as of ILOM 3.0.10” on page 148	• x86 system server SP • SPARC system server SP • CMM

Before You Begin

- Review the Power Monitoring Terminology defined in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide.*
- Review the conceptual information about Component Allocation Power Distribution in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide.*
- You must have ILOM 3.0.6 or later installed on your server or CMM. Where noted, some procedures described in this section require the server or CMM to be running ILOM 3.0.10 or later.
- As of ILOM 3.0.10, some of the CLI properties for the CMM and blades have changed:
  - `allocated_power` renamed to `granted_power`

- allocatable_power renamed to grantable_power
- permitted_power renamed to grant-in-aid

Where:

  - *Granted power* represents the sum of the maximum power consumed by either a single server component (such as, memory module), a category of server components (all memory modules), or a all server power consuming components.
  - *Grantable Power* indicates the total remaining power (watts) available from the CMM to allocate to blade slots without exceeding the grant limit.
  - *Grant Limit* represents the maximum power the system will grant to a blade slot.

- You must have Administrator (a) privileges in ILOM to change any power consumption or allocation configuration variables.

▼ View Server Power Allocations for All System Components

1. **Log in to the ILOM server SP CLI.**
2. **To view the sum of power allocated to all components in the system, type the following command:**

```
-> show /SP/powermgmt allocated_power
```

▼ View Server Component Power Allocations

1. **Log in to the ILOM server SP CLI.**
2. **To view power allocated to a component category (fans, CPUs, and so forth), type the following command:**

```
-> show /SP/powermgmt/powerconf/component_type
```

Where *component_type* is the name of the component category.

For example, to view the power allocated to all CPUs (component category), you would type:

```
-> show /SP/powermgmt/powerconf/CPUs
```

Note – For each command, the read-only value for the maximum power consumed by the component is returned, measured in watts.

3. **To view the power allocated to a specific component, type the following command:**

   -> **show /SP/powermgmt/powerconf/***component_type***/***component_name*

   - Where *component_type* is the name of the component category.
   - Where *component_name* is the name of the component.

   For example, to view the power allocated to a specific CPU, you would type:

   -> **show /SP/powermgmt/powerconf/CPUs/CPU***n*

   Where *n* is the installed location number of the CPU.

   Other rackmount server components can include:

   - **/SP/powermgmt/powerconf/Fans/FB0_FM***n*
   - **/SP/powermgmt/powerconf/PSUs/PS***n*
   - **/SP/powermgmt/powerconf/CPUs/MB_P***n*
   - **/SP/powermgmt/powerconf/memory/MB_P0_D***n*
   - **/SP/powermgmt/powerconf/IO/DBP_HDD***n*

   Other server module components can include:

   - **/SP/powermgmt/powerconf/CPUs/MB_P***n*
   - **/SP/powermgmt/powerconf/memory/MB_P0_D***n*
   - **/SP/powermgmt/powerconf/IO/DBP_HDD***n*

▼ View CMM Power Allocations for All Chassis Components

1. **Log in to the ILOM CMM CLI.**

2. **To view the sum of power allocated to all chassis system components, do one of the following:**

   - If you are running ILOM 3.0.8 or earlier, type the following command:

   -> **show** /**CMM/powermgmt allocated_power**

   - If you are running ILOM 3.0.10 or later, type the following command:

   -> **show** /**CMM/powermgmt granted_power**

3. **To view the remaining power available to allocate to blade slots, type the following command:**

   -> **show** /**CMM/powermgmt allocatable_power**

▼ View CMM Component Power Allocations

1. **Log in to the ILOM CMM CLI.**

2. **To view power allocated to a component category (fans, blade slots, and so forth), type the following command:**

   ```
   -> show /CMM/powermgmt/powerconf/component_type
   ```

   Where *component_type* is the name of the component category.

   For example, to view the power allocated to all blade slots (component category), you would type:

   ```
   -> show  /CMM/powermgmt/powerconf/bladeslots
   ```

Note – For each command, the read-only value for the maximum power consumed by the component is returned, measured in watts.

---

3. **To view the power allocated to a specific component, type the following command:**

   ```
   -> show  /CMM/powermgmt/powerconf/component_type/component_name
   ```

   Where *component_type* is the name of the component category.

   Where *component_name* is the name of the component.

   For example, to view the power allocated to a specific blade slot, you would type:

   ```
   ->  show  /CMM/powermgmt/powerconf/bladeslots/BLn
   ```

   Where *n* is the location number of the blade slot.

   Other CMM components can include:

   - **/CMM/powermgmt/powerconf/NEMs/NEM***n*
   - **/CMM/powermgmt/powerconf/Fans/FM***n*
   - **/CMM/powermgmt/powerconf/PSUs/PS***n*

▼ View Blade Slots Granted Power or Reserved Power as of ILOM 3.0.10

1. **Log in to the ILOM CMM CLI.**

2. **To view the sum of power granted to all blade slots or the sum of power reserved for all auto-powered I/O blade slots, type the following command:**

   ```
   -> show /CMM/powermgmt/powerconf/bladeslots
   ```

   The `granted_power` value and `reserved_power` value allocated to all blade slots appears, see example CLI output:

```
-> show /CMM/powermgmt/powerconf/bladeslots
/CMM/powermgmt/powerconf/bladeslots
    Targets:
        BL0
        BL1
        BL2
        BL3
        BL4
        BL5
        BL6
        BL7
        BL8
        BL9
Properties:
        granted_power = 952
        reserved_power = 876
Commands:
        cd
        show
```

▼ View Granted Power or Grant Limit for Blade as of ILOM 3.0.10

1. **Log into the ILOM CMM CLI.**

2. **To view the sum of power granted to an individual blade or to the grant limit value set for a blade, type the following command:**

   ```
   -> show /CMM/powermgmt/powerconf/bladeslot/BLn
   ```

   Where *n* represents the slot location for the blade.

   Example output:

```
 -> show /CMM/powermgmt/powerconf/bladeslots/BL1

  /CMM/powermgmt/powerconf/bladeslots/BL1
     Targets:

     Properties:
         granted_power = 0
         grant_limit = 800

     Commands:
         cd
         set
         show
```

Configuring Power Limit Properties

Topics

Description	Links	Platform Feature Support
Configure server SP power limit properties	• ”Configure Permitted Power for Blade Slots” on page 151 • ”Configure Server Power Budget Properties” on page 152 • ”Configure Grant Limit for aBlade as of ILOM 3.0.10” on page 154	• x86 system server SP • SPARC system server SP • CMM

Before You Begin

- Review the Power Monitoring Terminology defined in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide.*
- Review the conceptual information about Server Power Limit (or Server Power Budget) in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide.*
- You must have ILOM 3.0.6 or later installed on your server or CMM. Where noted, some procedures described in this section require the server or CMM to be running ILOM 3.0.10 or later.
- As of ILOM 3.0.10, some of the CLI properties for the CMM and blades have changed:
  - `allocated_power` renamed to `granted_power`
  - `allocatable_power` renamed to `grantable_power`
  - `permitted_power` renamed to `grant_limit`

  Where:

    - *Granted power* represents the sum of the maximum power consumed by either a single server component (such as a memory module), a category of server components (all memory modules), or a all server power consuming components.
    - *Grantable Power* indicates the total remaining power (watts) available from the CMM to allocate to blade slots without exceeding the grant limit.
    - *Grant Limit* represents the maximum power the system will grant to a blade slot.
- You must have Administrator (`a`) role privileges in ILOM to change any power management configuration variables.

▼ Configure Permitted Power for Blade Slots

1. **Log in to the ILOM CMM CLI.**
2. **To configure the permitted (maximum) power that the CMM will allocate to a blade slot, do one of the following:**
   - If you are using ILOM 3.0.8 or earlier, type the following command:

     ```
     -> set /CMM/powermgmt/powerconf/bladeslots/bladeslotn
     permitted_power=watts
     ```

     Where bladeslot*n* represents the blade slot that you want to configure.

     For example:

     ```
     -> set /CMM/powermgmt/powerconf/bladeslots/bladeslot1
     permitted_power=1200
     Set 'permitted_power' to '1200'
     ```

   - If you are using ILOM 3.0.10 or later, type the following command:

     ```
     -> set /CMM/powermgmt/powerconf/bladeslots/bladeslotn
     grant_limit=watts
     ```

     Where bladeslot*n* represents the blade slot that you want to configure.

Note – To prevent a server module from powering-on, set the permitted power value for the blade slot to 0.

▼ Configure Server Power Budget Properties

1. **Log in to the ILOM server SP CLI.**
2. **To view the current power budget settings, type the following command:**

   `-> `**`show /SP/powermgmt/budget`**

   Example output:

```
 /SP/powermgmt/budget
    Targets:

   Properties:
        activation_state = enabled
        status = ok
        powerlimit = 600 (watts)
        timelimit = default (30 seconds)
        violation_actions = none
        min_powerlimit = 150
        pendingpowerlimit = 600 (watts)
        pendingtimelimit = default
        pendingviolation_actions = none
        commitpending = (Cannot show property)
   Commands:
        cd
        show
->
```

3. **To configure power budget settings, type the following command:**

   `-> set /SP/powermgmt/budget` *property*=*value*

   Where *property*=*value* represents one of the following:

   - `activation_state=[enabled|disabled]`
   - `pendingpowerlimit=[`*watts*`w|`*percent*`%]`
   - `pendingtimelimit=[default|none|`*seconds*`]`
   - `pendingviolation_actions=[none|poweroff]`
   - `commitpending=true`

Power Budget Property	Description
Activation State	Enable this property to enable the power budget configuration.
Power Limit	Set a Power Limit in watts or as a percentage of the range between minimum and maximum system power. **Note -** The minimum system power is viewable in the CLI under the target /SP/powermgmt/budget min_powerlimit. The maximum system power is viewable from the Allocated Power property in the web interface or from the CLI under the target /SP/powermgmt allocated_power.
Time Limit	Specify one of the following grace periods for capping the power usage to the limit: • **Default** – Platform selected optimum grace period. • **None** – No grace period. Power capping is permanently applied. • **Custom** – User-specified grace period.
Violation Actions	The actions that the system will take if the power limit cannot be achieved within the grace period. This option can be set to None or Hard Power Off. This setting, by default, is set to None.

Note – To set the powerlimit, timelimit and violation_action in the ILOM CLI, you must set the matching pending properties and then commit these three pending properties as a group. After these properties are committed by typing set /SP/powermgmt/budget commitpending=true, the new values will apply whenever the budget activation_state is set to enabled.

For example:

```
-> set /SP/powermgmt/budget activation_state=enabled
Set 'activation_state' to 'enabled'
```

▼ Configure Grant Limit for aBlade as of ILOM 3.0.10

1. **Log in to the ILOM CMM CLI.**

Note – To change the grant power limit for any blade in ILOM requires an Admin (a) role user account.

---

2. **To configure the permitted (maximum) power that the CMM will allocate to a blade, type the following command:**

```
-> set /CMM/powermgmt/powerconf/bladeslots/BLn grant_limit=watts
```

Note – To prevent a server module from powering-on, set the grant limit value for the blade to `0`.

Note – The `grant_limit` value cannot be less than any amount already granted (`granted_power`).

Monitoring or Configuring CMM Power Supply Redundancy Properties

Topics

Description	Links	Platform Feature Support
Monitor or configure the CMM power supply redundancy properties	• "Monitor or Configure CMM Power Supply Redundancy Properties" on page 155	• CMM

Before You Begin

- Review the Power Monitoring Terminology defined in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide.*
- Review the conceptual information about power supply redundancy for CMM systems in the *Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide.*
- You must have ILOM 3.0.6 or later installed on your server to configure CMM power supply redundancy properties.
- You must have Administrator (a) role privileges in ILOM to change any power management configuration variables.

▼ Monitor or Configure CMM Power Supply Redundancy Properties

1. **Log in to the ILOM CMM CLI.**
2. **To configure power management settings, type the following command:**

   -> **set /CMM/powermgmt** *property***=***value*

   Where *property***=***value* represents the redundancy `[none|n+n]`

   For example:

```
-> set /CMM/powermgmt redundancy=none
Set 'redundancy' to 'none'
```

Note – When you change the redundancy policy, this change affects the amount of power the CMM is permitted to allocate to server modules (blades). The chassis `Permitted Power` is set to the power that the available power supplies can provide minus the redundant power that is available. In addition, when there is no redundant power available to the system, a loss of a power supply will cause the system to reduce the `Permitted Power`. If the system reduces the `Permitted Power` below the power that had already been allocated, you should immediately take steps to turn off the server modules to reduce the allocated power.

CHAPTER 10

Backing Up and Restoring ILOM Configuration

Topics

Description	Links
Back up the ILOM configuration	• "Back Up the ILOM Configuration" on page 158
Restore the ILOM configuration	• "Restore the ILOM Configuration" on page 160
Edit the backup XML file	• "Edit the Backup XML File" on page 162
Reset ILOM configuration to default settings	• "Reset the ILOM Configuration to Defaults" on page 164

Related Topics

For ILOM	Chapter or Section	Guide
• Concepts	• Configuration Management and Firmware Updates	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide* (820-6410)
• Web interface	• Backing Up and Restoring ILOM Configuration	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* (820-6411)
• IPMI and SNMP hosts	• Managing the ILOM Configuration	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide* (820-6413)

The ILOM 3.0 Documentation Collection is available at: `http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic`.

Backing Up the ILOM Configuration

Topics

Description	Links	Platform Feature Support
Back up your ILOM configuration	• "Back Up the ILOM Configuration" on page 158	• x86 system server SP • SPARC system server SP • CMM

Before You Begin

- Log in to the ILOM CLI as a user assigned the Admin, User Management, Console, Reset and Host Control, and Read Only (`a,u,c,r,o`) roles. These roles are required in order to perform a complete backup of the ILOM SP configuration.
- If you use a user account that does not have the roles listed above, the configuration backup file that is created might not include all of the ILOM SP configuration data.

▼ Back Up the ILOM Configuration

1. **Log in to the ILOM SP CLI or the CMM CLI.**

2. **Change to the** `/SP/config` **directory. Type:**

   -> **`cd /SP/config`**

3. **If you want sensitive data, such as user passwords, SSH keys, certificates, and so forth, to be backed up, you must provide a passphrase. Type:**

   -> **`set passphrase=`***passphrase*

4. **To initiate the Backup operation, type the following command from within the** `/SP/config` **directory:**

   -> **`set dump_uri=`**
   transfer_method`://`*username:password*`@`*ipaddress_or_hostname*`/`*directorypath*`/`*filename*

   Where:

   - *transfer_method* can be tftp, ftp, sftp, scp, http, or https.

- *username* is the name of the user account on the remote system. (*username* is required for scp, sftp, and ftp. *username* is not used for tftp, and it is optional for http and https.)
- *password* is the password for the user account on the remote system. (*password* is required for scp, sftp, and ftp. *password* is not used for tftp, and it is optional for http and https.)
- *ipaddress_or_hostname* is the IP address or the host name of the remote system.
- *directorypath* is the storage location on the remote system.
- *filename* is the name assigned to the backup file.

For example:

```
-> set dump_uri=
scp://adminuser:userpswd@1.2.3.4/Backup/Lab9/SP123.config
```

The Backup operation executes and you will be prompted when the operation completes. A Backup operation typically takes two to three minutes to complete.

Note – While the Backup operation is executing, sessions on the ILOM SP will be momentarily suspended. The sessions will resume normal operation once the Backup operation is complete.

Restoring the ILOM Configuration

Topics

Description	Links	Platform Feature Support
Restore the ILOM configuration	• "Restore the ILOM Configuration" on page 160	• x86 system server SP • SPARC system server SP • CMM

Before You Begin

- Log in to the ILOM CLI as a user assigned the Admin, User Management, Console, Reset and Host Control, and Read Only (`a,u,c,r,o`) roles. These roles are required to perform a complete restore of the ILOM SP configuration.
- When executing a Restore operation, use a user account that has the same or more privileges than the user account that was used to create the backup file; otherwise, some of the backed up configuration data might not be restored. All

configuration properties that are not restored appear in the event log. Therefore, one way to verify whether all the configuration properties were restored is to check the event log.

▼ Restore the ILOM Configuration

1. **Log in to the ILOM SP CLI or the CMM CLI.**
2. **Change to the `/SP/config` directory. Type:**

   -> **`cd /SP/config`**

3. **If a passphrase was specified when the backup file was created, you must specify the same passphrase to perform the Restore operation. Type:**

   -> **`set passphrase=`***passphrase*

   The passphrase must be the same passphrase that was used when the backup file was created.

4. **To initiate the Restore operation, type the following:**

   -> **`set load_uri=`**
   transfer_method`://`*username:password*`@`*ipaddress_or_hostname*`/`*directorypath*`/`*filename*

   Where:

   - *transfer_method* can be tftp, ftp, sftp, scp, http, or https.
   - *username* is the name of the user account on the remote system. (*username* is required for scp, sftp, and ftp. *username* is not used for tftp, and it is optional for http and https.)
   - *password* is the password for the user account on the remote system. (*password* is required for scp, sftp, and ftp. *password* is not used for tftp, and it is optional for http and https.)
   - *ipaddress_or_hostname* is the IP address or the host name of the remote system.
   - *directorypath* is the storage location on the remote system.
   - *filename* is the name assigned to the backup file.

   For example:

   ```
   -> set load_uri=
   scp://adminuser:userpswd@1.2.3.4/Backup/Lab9/SP123.config
   ```

The Restore operation executes. The XML file is parsed. A Restore operation typically takes two to three minutes to complete.

Note – While the Restore operation is executing, sessions on the ILOM SP will be momentarily suspended. The sessions will resume normal operation once the Restore operation is complete.

Edit the Backup XML file

Topics

Description	Links	Platform Feature Support
Edit the backup XML file	• "Edit the Backup XML File" on page 162	• x86 system server SP • SPARC system server SP • CMM

Before You Begin

- Before you use a backed up XML file on another system, you should edit the file to remove any information that is unique to a particular system, for example, the IP address.

▼ Edit the Backup XML File

The following is an example of a backed up XML file. The contents of the file are abbreviated for the example used in this procedure.

```
<SP_config version="3.0">
<entry>
<property>/SP/check_physical_presence</property>
<value>false</value>
</entry>
<entry>
<property>/SP/hostname</property>
<value>labysystem12</value>
</entry>
<entry>
<property>/SP/system_identifier</property>
<value>SUN BLADE X8400 SERVER MODULE, ILOM v3.0.0.0, r32722
</value>
</entry>
.
.
.
<entry>
<property>/SP/clock/datetime</property>
<value>Mon May 12 15:31:09 2008</value>
</entry>
.
.
.
<entry>
<property>/SP/config/passphrase</property>
<value encrypted="true">89541176be7c</value>
</entry>
.
.
.
<entry>
<property>/SP/network/pendingipaddress</property>
<value>1.2.3.4</value>
</entry>
.
.
.
<entry>
<property>/SP/network/commitpending</property>
<value>true</value>
</entry>
.
```

```
.
.
<entry>
<property>/SP/services/snmp/sets</property>
<value>enabled</value>
</entry>
.
.
.
<entry>
<property>/SP/users/john/role</property>
<value>aucro</value>
</entry>
<entry>
<entry>
<property>/SP/users/john/password</property>
<value encrypted="true">c21f5a3df51db69fdf</value>
</entry>
</SP_config>
```

1. **Consider the following in the example XML file:**
   - The configuration settings, with exception of the password and the passphrase, are in clear text.
   - The `check_physical_presence` property, which is the first configuration entry in the file, is set to `false`. The default setting is `true` so this setting represents a change to the default ILOM configuration.
   - The configuration settings for `pendingipaddress` and `commitpending` are examples of settings that should be deleted before you use the backup XML file for a Restore operation because these settings are unique to each server.
   - The user account `john` is configured with the `a,u,c,r,o` roles. The default ILOM configuration does *not* have any configured user accounts so this account represents a change to the default ILOM configuration.
   - The SNMP `sets` property is set to enabled. The default setting is disabled.
2. **To modify the configuration settings that are in clear text, change the values or add new configuration settings.**

   For example:
   - To change the roles assigned to the user `john`, change the text as follows:

```
<entry>
<property>/SP/users/john/role</property>
<value>auo</value>
</entry>
<entry>
```

- To add a new user account and assign that account the a,u,c,r,o roles, add the following text directly below the entry for user john:

```
<entry>
<property>/SP/users/bill/role</property>
<value>aucro</value>
</entry>
<entry>
```

- To change a password, delete the encrypted="true" setting and the encrypted password string and enter the password in plain text. For example, to change the password for the user john, change the text as follows:

```
<entry>
<property>/SP/users/john/password</property>
<value>newpassword</value>
</entry>
```

3. **After you have made the changes to the backup XML file, save the file so that you can use it for a Restore operation on the same system or a different system.**

Resetting the ILOM Configuration

Topics

Description	Links	Platform Feature Support
Reset the ILOM configuration to the default settings	• "Reset the ILOM Configuration to Defaults" on page 164	• x86 system server SP • SPARC system server SP • CMM

Before You Begin

- To reset the ILOM configuration to the default settings, you need the Admin (a) role enabled.

▼ Reset the ILOM Configuration to Defaults

1. **Log in to the ILOM SP CLI or the CMM CLI.**

2. **Change to the `/SP` directory, type:**

   ```
   -> cd /SP
   ```

3. **Type one of the following commands, depending on the option you select to reset the default settings.**

   - If you want to reset the ILOM configuration using the `all` option, type:

     ```
     -> set reset_to_defaults=all
     ```

     On the next reboot of the ILOM SP, the ILOM configuration default settings are restored.

   - If you want to reset the ILOM configuration using the `factory` option, type:

     ```
     -> set reset_to_defaults=factory
     ```

     On the next reboot of the ILOM SP, the ILOM configuration default settings are restored and the log files are erased.

   - If you want to cancel a reset operation just previously specified, type:

     ```
     -> set reset_to_defaults=none
     ```

     The previously issued `reset_to_defaults` command is canceled provided the `reset_to_defaults=none` command is issued before the ILOM SP reboots.

CHAPTER 11

Updating ILOM Firmware

Topics

Description	Links
Review the prerequisites	• "Before You Begin" on page 169
Update ILOM firmware	• "Identify ILOM Firmware Version" on page 169 • "Download New ILOM Firmware Image" on page 169 • "Update the Firmware Image" on page 170
Troubleshoot network problem during firmware update	• "Recover From a Network Failure During Firmware Update" on page 172
Reset the ILOM SP	• "Reset ILOM SP or CMM" on page 173

Related Topics

For ILOM	Chapter or Section	Guide
• Concepts	• Configuration Management and Firmware Updates	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide* (820-6410)
• Web interface	• Updating ILOM Firmware	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* (820-6411)
• IPMI and SNMP hosts	• Configuring ILOM Firmware Settings	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Management Protocols Reference Guide* (820-6413)
• CLI and Web interface (CMM only)	• Firmware Update Procedures	*Oracle Integrated Lights Out Manager (ILOM) CMM Administration Guide for Sun Blade 6000 and Sun Blade 6048 Modular Systems* (820-0052)

The ILOM 3.0 Documentation Collection is available at: `http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic`.

Updating the ILOM Firmware

Topics

Description	Links	Platform Feature Support
Review the prerequisites	• "Before You Begin" on page 169	• x86 system server SP • SPARC system server SP • CMM
Identify the current ILOM firmware version	• "Identify ILOM Firmware Version" on page 169	
Download the firmware for your system	• "Download New ILOM Firmware Image" on page 169	
Update the firmware image	• "Update the Firmware Image" on page 170	
Troubleshoot network problem during firmware update	• "Recover From a Network Failure During Firmware Update" on page 172	

Before You Begin

Prior to performing the procedures in this section, the following requirements must be met:

- Identify the version of ILOM that is currently running on your system.
- Download the firmware image for your server or CMM from the Oracle's Sun platform product web site and place the image on your TFTP, FTP, or HTTP server.
- If required by your platform, shut down your host operating system before updating the firmware on your server SP.
- Obtain an ILOM user name and password that has Admin (a) role account privileges. You must have Admin (a) privileges to update the firmware on the system.
- The firmware update process takes several minutes to complete. During this time, do not perform other ILOM tasks. When the firmware update is complete, the system will reboot.

Note – As of ILOM 3.0.10, a new feature is available to manage firmware updates for Oracle Sun Modular System chassis components. For information and procedures for updating ILOM firmware on CMM chassis components, refer to the *Oracle Integrated Lights Out Manager (ILOM) CMM Administration Guide for Sun Blade 6000 and Sun Blade 6048 Modular Systems* (820-0052).

▼ Identify ILOM Firmware Version

Follow these steps to identify the ILOM firmware version:

1. **Log in to the ILOM SP CLI or the CMM CLI.**

2. **At the command prompt, type** `version`**.**

   The following information appears:

```
SP firmware 3.0.0.1
SP firmware build number: #####
SP firmware date: Fri Nov 28 14:03:21 EDT 2008
SP filesystem version: 0.1.22
```

▼ Download New ILOM Firmware Image

1. **Navigate to** `http://www.oracle.com/us/products/servers-storage/servers/index.html`**.**

2. **Expand the “Downloads” box at the right of the page, then click the “Drivers and Firmware” link.**

3. **Navigate to the appropriate page for your Sun server.**

4. **Select the “Downloads and Firmware” tab.**

5. **Click the “Download” link that is appropriate for your server.**

▼ Update the Firmware Image

Note – If required by your platform, shut down your host operating system before updating the firmware on your server SP.

Note – To gracefully shut down your host operating system, use the `Remote Power Controls` -> `Graceful Shutdown and Power Off` option in the ILOM web interface, or issue the `stop /SYS` command from the ILOM CLI.

---

1. **Log in to the ILOM SP CLI or the CMM CLI.**

2. **Verify that you have network connectivity to update the firmware.**

   For example:

   - To verify network connectivity on a server SP, type:

     ```
     -> show /SP/network
     ```

   - To verify network connectivity on a CMM, type:

     ```
     -> show /CMM/network
     ```

3. **Type the following command to load the ILOM firmware image:**

   ```
   -> load -source <supported_protocol>://<server_ip>/<path_to_firmware_image>/
   <filename.xxx>
   ```

   A note about the firmware update process followed by message prompts to load the image are displayed. The text of the note depends on your server platform.

4. **At the prompt for loading the specified file, type `y` for yes or `n` for no.**

   The prompt to preserve the configuration appears.

   For example:

   ```
   Do you want to preserve the configuration (y/n)?
   ```

5. **At the preserve configuration prompt, type `y` for yes or `n` for no.**

   Type `y` to save your existing ILOM configuration and to restore that configuration when the update process completes.

Note – Typing `n` at this prompt will advance you to another platform-specific prompt.

---

6. **Perform one of the following actions:**

   - If you have a **2.x firmware release installed** on your system, the system loads the specified firmware file then automatically reboots to complete the firmware update. **Proceed to Step 7**.
   - If you have a **3.x firmware release installed** on a **SPARC system**, the system loads the specified firmware file then automatically reboots to complete the firmware update. **Proceed to Step 7**.
   - If you have a **3.x firmware release installed** on an **x86 system**, a prompt to postpone the BIOS update appears. For example:

     ```
     Do you want to force the server off if BIOS needs to be upgraded
     (y/n)?
     ```

   a. **At the prompt to postpone the BIOS update, type `y` for yes or `n` for no.**

      The system loads the specified firmware file then automatically reboots to complete the firmware update.

Note – The BIOS prompt only appears on x86 systems currently running ILOM 3.x firmware release. If you answer yes (`y`) to the prompt, the system postpones the BIOS update until the next time the system reboots. If you answer no (`n`) to the prompt, the system automatically updates the BIOS, if necessary, when updating the firmware.

Note – The BIOS default settings cannot be preserved when updating the SP firmware. After updating the SP firmware, the default settings are automatically loaded for the new BIOS image.

---

   b. **Proceed to Step 7.**

7. **Reconnect to the ILOM server SP or CMM using an SSH connection and using the same user name and password that you provided in Step 1 of this procedure.**

Note – If you did not preserve the ILOM configuration before the firmware update, you will need to perform the initial ILOM setup procedures to reconnect to ILOM.

8. **Verify that the proper firmware version was installed. At the CLI prompt, type:**

```
-> version
```

The firmware version on the server SP or CMM should correspond with the firmware version you installed.

▼ Recover From a Network Failure During Firmware Update

Note – If you were performing the firmware update process and a network failure occurs, ILOM will automatically time-out and reboot the system.

1. **Address and fix the network problem.**
2. **Reconnect to the ILOM SP.**
3. **Restart the firmware update process.**

Resetting the ILOM SP or CMM

Topics

Description	Links	Platform Feature Support
Reset ILOM service processor	• "Reset ILOM SP or CMM" on page 173	• x86 system server SP • SPARC system server SP

Before You Begin

- To reset the SP, you need the Reset and Host Control (`r`) role enabled.
- After updating the ILOM/BIOS firmware, you must reset the ILOM SP or CMM.

If you need to reset your ILOM service processor (SP), you can do so without affecting the host OS. However, resetting an SP disconnects your current ILOM session and renders the SP unmanageable during reset.

▼ Reset ILOM SP or CMM

1. **Log in to the ILOM server SP CLI or the ILOM CMM CLI.**
2. **Use the reset command to boot the power on the server SP or CMM.**

   For example:

   ```
   -> reset /SP
   ```

   or

   ```
   -> reset /CMM
   ```

   The SP or CMM resets and reboots.

CHAPTER 12

Managing Remote Hosts Storage Redirection and Securing the ILOM Remote Console

Topics

Description	Links
Set up storage redirection to redirect storage devices	• "Performing the Initial Setup Tasks for Storage Redirection" on page 176 • "Launch Storage Redirection CLI Using a Command Window or Terminal" on page 185
Configure the ILOM Remote Console Lock option	• "Securing the ILOM Remote Console" on page 192

Related Topics

For ILOM	Chapter or Section	Guide
• Concepts	• Remote Host Management Options	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide* (820-6410)
• Web interface	• Managing Remote Hosts Redirection and Securing the ILOM Remote Console	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* (820-6411)
The ILOM 3.0 Documentation Collection is available at: `http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic`.		

Performing the Initial Setup Tasks for Storage Redirection

Step	Task	Description	Platform Feature Support
1	Ensure that all requirements are met prior to performing the initial setup procedures in this section.	• "Before You Begin" on page 176	• x86 system server SP • SPARC system server SP
2	Start the Storage Redirection Service on your system.	• "Start Storage Redirection Service Using Mozilla Firefox Web Browser" on page 177 - or- • "Start Storage Redirection Service Using Internet Explorer (IE) Web Browser" on page 180	
3	Download and install the Storage Redirection Client.	• "Download and Install the Storage Redirection Client" on page 182.	

Note – The Storage Redirection CLI in ILOM 3.0 is supported on all of Oracle's Sun x86 processor-based servers, as well as some SPARC processor-based servers. This feature is not supported on chassis monitoring modules (CMMs) or x86 processor-based servers running ILOM 2.0.

Before You Begin

Prior to setting up your system for storage redirection, the following prerequisites must be met.

- A connection is established from your local system to a remote host server SP ILOM web interface.
- Server module SP must be running ILOM 3.0 or later.

- The Java runtime environment (1.5 or later) is installed on your local system. To download the latest Java runtime environment, see `http://java.com.`

Note – If you do not have `JAVA_HOME` environment configured on your desktop, you might need to enter the full path

---

- The 32-bit Java Development kit (JDK) file needs to be specified when starting the Storage Redirection Service. You can choose (as described in the procedures) to initially save this file to disk and subsequently run this service directly from the command-line interface or you can choose to initially open the file with the default application and subsequently start the service from the ILOM web interface prior to using the Storage Redirection properties from the CLI.
- Any user with a valid user account in ILOM can start or install the Storage Redirection Service or Client on his or her local system. However, after the initial setup for the Storage Redirection CLI is complete, you will be required to enter a valid Admin (`a`) or Console (`c`) role account to start or stop the redirection of a storage device (CD/DVD, or ISO image) on a remote server.
- The default network communication port provided for Storage Redirection CLI is 2121. This default socket port enables the Storage Redirection CLI to communicate over the network with a remote host server SP. If you need to change the default network port, you must edit the `Jnlpgenerator-cli` file to manually override the default port number (2121). For instructions for changing this port, see "View and Configure Serial Port Settings" on page 43.

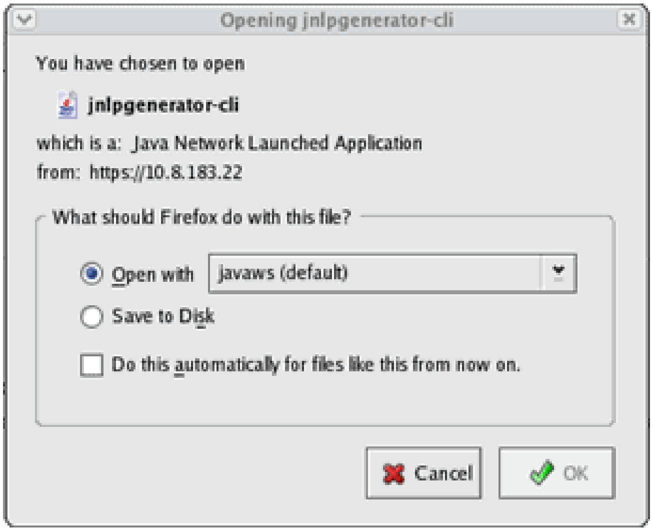
▼ Start Storage Redirection Service Using Mozilla Firefox Web Browser

Follow these steps to specify the 32-bit JDK when starting the service for the Storage Redirection CLI using the Mozilla Firefox web browser.

1. **Log in to the ILOM SP web interface.**

2. **Click Remote Control --> Redirection--> Launch Service.**

A dialog appears indicating the file type chosen to start the service.



Opening jnlpgenerator-cli

You have chosen to open

jnlpgenerator-cli

which is a: Java Network Launched Application

from: https://10.8.183.22

What should Firefox do with this file?

● Open with javaws (default)

○ Save to Disk

□ Do this automatically for files like this from now on.

3. **In the Opening jnlpgenerator-cli file dialog, do the following:**

   a. **Specify one of the following options for accessing the 32-bit JDK file.**

      - **Save to Disk** —To save the `jnlpgenerator-cli` file on your local system and run the service directly from a command line, select `Save it to disk` then click `OK`.

        If you select this option, you will *not* need to subsequently sign in to the ILOM web interface to start the service. You will be able to start the service directly from a command window or terminal.

      - **Open with...** —To run the service directly from the ILOM web interface, select `Open it with javaws (default)`(32-bit JDK file) then click `OK`.

        If you select this option, the `jnlp` file is not saved on your local system and you will need to subsequently sign in to the ILOM web interface to start the service prior to launching the Storage Redirection CLI.

   b. **(Optional) Select the check box for** `Do this automatically for files like this from now on` **then click OK.**

Note – To prevent the `Opening Jnlpgenerator-cli dialog` from reappearing each time you start the service from the ILOM web interface, you can select (enable) the check box for `Do this automatically for files like this from now on.` However, if you choose to enable this option, you will no longer be able to display this dialog when starting the service or installing the service from the ILOM web interface.

Note – If, in the future, you need to modify the default communication port number (2121) shipped with the Storage Redirection feature, you will need to display the `Opening Jnlpgenerator-cli` dialog to save and edit the `jnlpgenerator-cli` file on your system. In this instance, it is not recommended that you select (enable) the option for `Always perform this action when handling files of this type`. For more information about changing the default port number, see "View and Configure Serial Port Settings" on page 43.

---

4. Perform one of the following actions:

If you chose in Step 3-a to:	Perform these steps:
Save the `jnlpgenerator-cli` file	1. In the Save As dialog, save the `jnlpgenerator-cli` file to a location on your local system. 2. To start the service from the command line, open a command window or terminal. 3. Navigate to the location where the `jnlpgenerator-cli` file is installed, then issue the `javaws rconsole.jnlp` command to start the service. For example: `->` **`cd`** *<jnlp file location>***`javaws rconsole.jnlp`**
- OR -	
Run the service directly from the web interface	• In the Warning Security dialog, click Run to start the Storage Redirection service.

Start Storage Redirection Service Using Internet Explorer (IE) Web Browser

Perform the following steps **prior to starting the service for the Storage Redirection CLI** feature in ILOM. These steps describe how to start the Storage Redirection Service after registering the 32-bit JDK file.

1. **Prior to starting the Storage Redirection Service on your Windows system for the first time, you must register the 32-bit JDK file by following these steps:**

   a. **On the Windows client, open Windows Explorer (not Internet Explorer).**

   b. **In the Windows Explorer dialog, select** `Tools` **-->** `Folder Options` **then select the Files Types tab.**

   c. **In the Files Types tab, do the following:**

      -- In the registered file type list, select the JNLP file type and click Change.

      -- In the `Open With...` dialog, click `Browse` to select the 32-bit JDK file.

      -- Select the check box for `Always use the selected program to open this kind of file`.

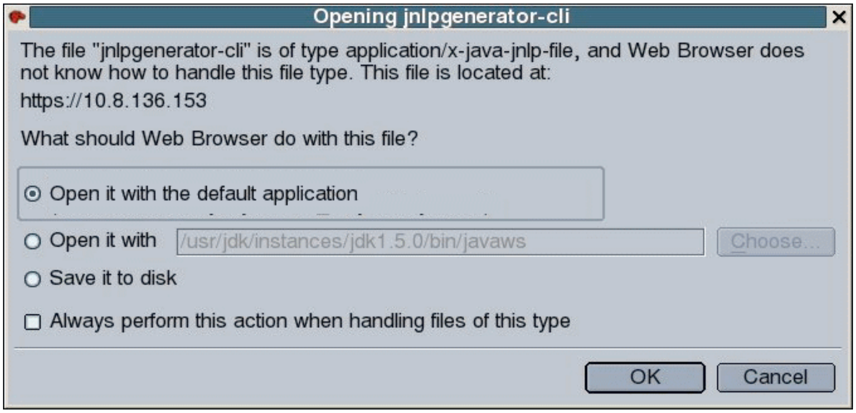
      -- Click `OK`, then start the service for Storage Redirection in the ILOM web interface.

2. **To start the Storage Redirection Service (after registering the 32-bit JDK file), do the following:**

   a. **Log in to the ILOM SP web interface.**

   b. **Click Remote Control --> Redirection--> Launch Service.**

   The Opening Jnlpgenerator-cli dialog appears.



Opening jnlpgenerator-cli

The file "jnlpgenerator-cli" is of type application/x-java-jnlp-file, and Web Browser does not know how to handle this file type. This file is located at:
https://10.8.136.153

What should Web Browser do with this file?

● Open it with the default application

○ Open it with /usr/jdk/instances/jdk1.5.0/bin/javaws

○ Save it to disk

□ Always perform this action when handling files of this type

c. **In the Opening Jnlpgenerator-cli dialog, perform one of the following actions:**

- **Save it to disk** —To save the `jnlpgenerator-cli` file on your local system and run the service directly from a command line, select `Save it to disk` then click `OK`.

  If you select this option, you will *not* need to subsequently sign in to the ILOM web interface to start the service. You will be able to start the service directly from a command window or terminal.

- **Open with...** — To run the service directly from the ILOM web interface, select `Open it with the` javaws `(default)` (32-bit JDK file) then click `OK`.

  If you select this option, the `jnlp` file is not saved on your local system and you will need to subsequently sign in to the ILOM web interface to start the service prior to launching the Storage Redirection CLI.

Note – To prevent the `Opening Jnlpgenerator-cli  dialog` from reappearing each time you start the service from the ILOM web interface, you can select (enable) the check box for `Always perform this action when handling files of this type`. However, if you choose to enable this option, you will no longer be able to display this dialog when starting the service or installing the service from the ILOM web interface.

Note – If, in the future, you need to modify the default communication port number (2121) shipped with the Storage Redirection feature, you will need to display the `Opening Jnlpgenerator-cli` dialog to save and edit the `jnlpgenerator-cli` file on your system. In this instance, it is not recommended that you select (enable) the option for `Always perform this action when handling files of this type`. For more information about changing the default port number, see ”View and Configure Serial Port Settings” on page 43.

---

d. Perform one of the following actions:

If you chose in Step C to:	Perform these steps:
Save the `jnlpgenerator-cli` file	1. In the Save As dialog, save the `jnlpgenerator-cli` file to a location on your local system. 2. To start the service from the command line, open a command window or terminal. 3. Navigate to the location where the `jnlpgenerator-cli` file is installed, then issue the `javaws rconsole.jnlp` command to start the service. For example: `->` **`cd`** *<jnlp file location>*`javaws rconsole.jnlp`
- OR -	
Run the service directly from the web interface	• In the Warning Security dialog, click Run to start the Storage Redirection service.

If the Storage Redirection service fails to start, an error message appears informing you of an error condition. Otherwise, if an error message did not appear, the service is started and is waiting for user input.

▼ Download and Install the Storage Redirection Client

Follow these steps to download and install the Storage Redirection client on your local system.

Note – The Storage Redirection client is a one-time client installation.

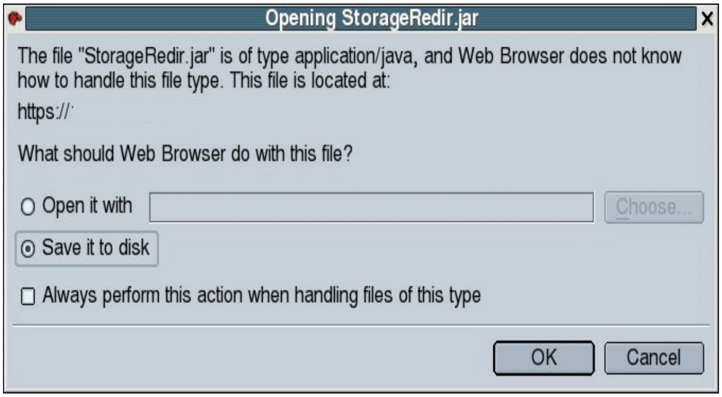
---

1. **In the ILOM SP web interface, select Remote Control --> Redirection.**

   The Launch Redirection page appears.

2. **Click** `Download Client`**.**

   The Opening StorageRedir.jar dialog appears.



Opening StorageRedir.jar

The file "StorageRedir.jar" is of type application/java, and Web Browser does not know how to handle this file type. This file is located at:

https://

What should Web Browser do with this file?

○ Open it with

● Save it to disk

□ Always perform this action when handling files of this type

3. **In the Opening StorageRedir.jar dialog, click** `Save it to Disk`, **then click** `OK`**.**

   The Save As dialog appears.

Note – If you do not want the `Opening StorageRedir` dialog to reappear when installing the `.jar` file on other remote clients, you can select (enable) the check box for `Always perform this action when handling files of this type`. However, if you choose to enable this option, you will no longer be able to display this dialog (`Opening StorageRedir`) in the future when downloading the `.jar` file.

---

4. **In the Save As dialog, save the** `StorageRedir.jar` **file to a location on your local system.**

Launching the Storage Redirection CLI to Redirect Storage Devices

Step	Task	Links	Platform Feature Support
1	Ensure that all requirements are met before using the Storage Redirection CLI	• "Before You Begin" on page 184	• x86 system server SP • SPARC system server SP
2	Launch the Storage Redirection CLI	• "Launch Storage Redirection CLI Using a Command Window or Terminal" on page 185	
3	If applicable, verify that Storage Redirection Service is running	• "Verify the Storage Redirection Service Is Running" on page 187	
4	If applicable, display command-line Help; or learn more about the Storage Redirection command-line modes, syntax, and usage	• "Display Storage Redirection CLI Help Information" on page 187	
5	Redirect a storage device from the CLI	• "Start Redirection of Storage Device" on page 188	
6	View a list of active storage devices	• "View Active Storage Redirections" on page 189	
7	Stop the redirection of a storage device	• "Stop Redirection of Storage Device" on page 190	

Before You Begin

The following requirements must be met prior to performing the procedures in this section.

- The Storage Redirection Service must be started on your local system. If you installed the service on your local system, you can start it from a command window or terminal. If you did not install the service on your local system, you must start it from the ILOM web interface. For information about how to start or install the Storage Redirection service, see ”Start Storage Redirection Service Using Mozilla Firefox Web Browser” on page 177.

- The Storage Redirection client (`StorageRedir.jar`) must be installed on your local system. For more information about how to install the Storage Redirection client, see ”Download and Install the Storage Redirection Client” on page 182.
- The Java runtime environment (1.5 or later) must be installed on your local system. To download the latest Java runtime environment, see `http://java.com.`
- A valid Admin (`a`) or Console (`c`) role account in ILOM is required to start or stop the redirection of a storage device (CD/DVD, or ISO image) on a remote server. For more information about user accounts and roles, see ”Assign Roles to a User Account” on page 61.

Note – Any user with a valid user account in ILOM can launch the Storage Redirection CLI (from a command window or terminal) and verify the status of the the service, or view the occurrence of an active storage redirection.

- On Windows systems, both uppercase letter 'C:\' and lowercase letter 'c:\' are accepted for cdrom and floppy image redirection. However, only uppercase letter ('D:\', 'A:\') are accepted for both cdrom drive and floppy drive redirection.
- For more information about the Storage Redirection command-line modes, syntax and usage, see “Storage Redirection Command-Line Modes, Syntax, and Usage” on page 251.

▼ Launch Storage Redirection CLI Using a Command Window or Terminal

---

Note – Prior to launching the Storage Redirection CLI, you must have started the Storage Redirection Service. For instructions for launching the service, see ”Start Storage Redirection Service Using Mozilla Firefox Web Browser” on page 177.

---

1. **Open a command-line interface.**

   For example:

   - Windows systems: Click Run from the Start menu and type `cmd,` then click `OK`.
   - Solaris or Linux systems: Open a terminal window on the desktop.

2. **Perform one of the following actions:**

   - To enter commands from an **interactive shell mode**, do the following:

a. **In the command-line interface, navigate to the directory where the Storage Redirection client (**`StorageRedir.jar`**) was installed using the** `cd` **command.**

For example:

```
cd <my_settings>/<storage_redirect_directory>
```

b. **At the directory prompt, enter the following command to launch the Storage Redirection CLI.**

```
java -jar StorageRedir.jar
```

For example:

```
C:\Documents and Settings\<redirectstorage>java -jar StorageRedir.jar
```

The `<storageredir>` prompt appears.

Note – If you are using Windows, you must specify an uppercase letter for target drive directory. For example, if you are using an `C`drive location, you need to specify `C:\` instead of `c:\`.

- To enter commands from an **non-interactive shell mode,** do the following:

a. **In the command-line interface, enter the command to launch the Storage Redirection CLI** (`java -jar StorageRedir.jar`) **at the shell prompt** (`$`).

```
$ java -jar StorageRedir.jar
```

Note – If you do not have a `JAVA_HOME` environment configured, you might need to use the full path to your Java binary. For example, if your JDK package was installed under `/home/`*user_name*`/jdk` then you would type:
`/home/`*user_name*`/jdk/bin/java -jar ...`

Note – If the Storage Redirection CLI fails to launch, a detailed error message appears explaining the error condition. Otherwise, the Storage Redirection CLI is ready for user input.

▼ Verify the Storage Redirection Service Is Running

Note – The following procedure assumes that you have already launched the Storage Redirection CLI from a command window or terminal. For instructions for launching the Storage Redirection CLI, see "Launch Storage Redirection CLI Using a Command Window or Terminal" on page 185.

- **At the** `<storageredir>` **prompt, type the following command to verify that the Storage Redirection service is active:**

  ```
  test-service
  ```

  For example:

  ```
  <storageredir> test-service
  ```

  Alternatively, you could enter this same command (`test-service`) using the non-interactive shell mode syntax. For more information, see "Storage Redirection Command-Line Modes, Syntax, and Usage" on page 251.

  A message appears stating whether the service connection passed or failed.

Note – If the service connection fails, you will need to start the Storage Redirection Service from the ILOM web interface or from a command window (if the service was installed) by issuing the `javaws rconsole.jnlp` command. For details, see "Start Storage Redirection Service Using Mozilla Firefox Web Browser" on page 177.

▼ Display Storage Redirection CLI Help Information

Note – The following procedure assumes that you have already launched the Storage Redirection CLI from a command window or terminal. For instructions for launching the Storage Redirection CLI, see "Launch Storage Redirection CLI Using a Command Window or Terminal" on page 185.

- **At the** `<storageredir>` **prompt, type the following command to display the command-line help:**

  ```
  help
  ```

  For example:

```
<storageredir> help
```

The following information about the command syntax and usage appears:

```
Usage:
          list [-p storageredir_port] [remote_SP]
          start -r redir_type -t redir_type_path
            -u remote_username [-s remote_user_password]
            [-p storageredir_port] remote_SP
          stop -r redir_type -u remote_username
           [-s remote_user_password] [-p storageredir_port] remote_SP
          stop-service [-p storageredir_port]
          test-service [-p storageredir_port]
          help
          version
          quit
```

Alternatively, you could enter this same command (`help`) using the non-interactive shell mode syntax. For more information, see "Storage Redirection Command-Line Modes, Syntax, and Usage" on page 251.

▼ Start Redirection of Storage Device

Note – The following procedure assumes that you have already launched the Storage Redirection CLI from a command window or terminal. For instructions for launching the Storage Redirection CLI, see "Launch Storage Redirection CLI Using a Command Window or Terminal" on page 185.

Note – Commands shown in the following procedure should be entered as one continuous string.

Note – On Windows systems, both uppercase letter 'C:\' and lowercase letter 'c:\' are accepted for cdrom and floppy image redirection. However, only uppercase letter ('D:\', 'A:\') are accepted for both cdrom drive and floppy drive redirection.

- **At the `<storageredir>` prompt, type the `start` command followed by the commands and properties for the *redirection device type, path to device, remote SP user_name and password*, and the *IP address* of the remote SP.**

  For example:

```
<storageredir> start -r redir_type -t redir_type_path -u remote_username [-
s remote_user_password] [-p non_default_storageredir_port] remote_SP_IP
```

Note – If you are using Windows, you must specify an uppercase letter for the drive path. For example, if you are using an `A` drive location, you need to specify `A:\` instead of `a:\` in the drive path.

Alternatively, you could enter this same command (`start`) using the non-interactive shell mode syntax. For more information, see "Storage Redirection Command-Line Modes, Syntax, and Usage" on page 251.

Note – You must specify a valid Admin or Console role account (`-u` *remote_username* `[-s` *remote_user_password*`])` to start the redirection of a storage device on a remote server. If you do not specify the password command (`-s` *remote_user_password*), the system will automatically prompt you for it.

View Active Storage Redirections

Note – The following procedure assumes that you have already launched the Storage Redirection CLI from a command window or terminal. For instructions for launching the Storage Redirection CLI, see "Launch Storage Redirection CLI Using a Command Window or Terminal" on page 185.

- **At the** `<storageredir>` **prompt, type the** `list` **command followed by the sub-commands and properties for any non-default storage redirection** ***port(s)*** **and the** ***IP address(es)*** **of the remote host server SP.**

  For example:

  ```
  <storageredir> list [-p non_default _storageredir_port] remote_SP
  ```

  Alternatively, you could enter this same command (`list`) using the non-interactive shell mode syntax. For more information, see "Storage Redirection Command-Line Modes, Syntax, and Usage" on page 251.

  A list appears identifying the active storage redirections for each server SP specified.

▼ Stop Redirection of Storage Device

Note – The following procedure assumes that you have already launched the Storage Redirection CLI from a command window or terminal. For instructions for launching the Storage Redirection CLI, see ”Launch Storage Redirection CLI Using a Command Window or Terminal” on page 185.

Note – Commands shown in the following procedure should be entered as one continuous string.

- **At the `<storageredir>` prompt, type the `stop` command followed by the commands and properties for the: *storage device type*, *remote SP user name* and *password*, *storage redirection port* and the *IP address* of the remote host server SP.**

  For example:

  ```
  <storageredir> stop -r redir_type -u remote_username [-s
  remote_user_password] [-p non_defult_storageredir_port] remote_SP
  ```

  Alternatively, you could enter this same command (`stop`) using the non-interactive shell mode syntax. For more information, see “Storage Redirection Command-Line Modes, Syntax, and Usage” on page 251.

Note – You must specify a valid Admin or Console role account (`-u` *remote_username* `[-s` *remote_user_password*`]`) to stop the redirection of a storage device on a remote server. If you do not specify the password command (`-s` *remote_user_password*) the system will automatically prompt you for it.

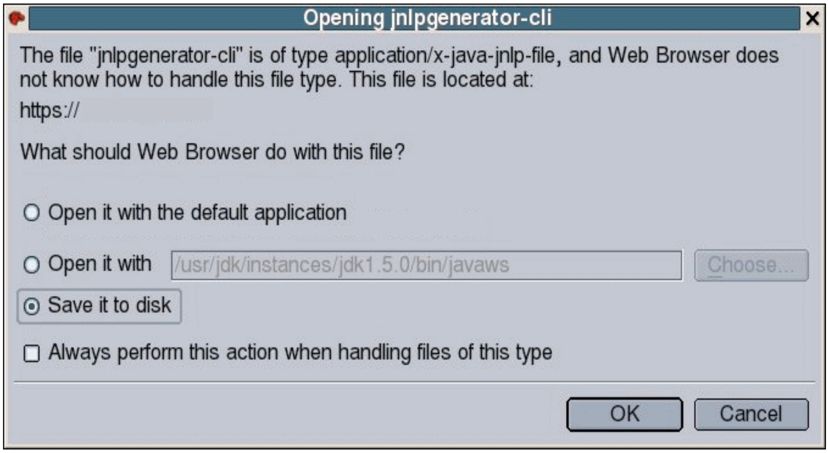
▼ Change the Default Storage Redirection Network Port: 2121

1. **In the ILOM SP web interface, select Remote Control --> Redirection.**

   The Launch Redirection page appears.

2. **Click `Launch Service`.**

   The Opening Jnlpgenerator-cli dialog appears.



Opening jnlpgenerator-cli

The file "jnlpgenerator-cli" is of type application/x-java-jnlp-file, and Web Browser does not know how to handle this file type. This file is located at:

https://

What should Web Browser do with this file?

○ Open it with the default application

○ Open it with /usr/jdk/instances/jdk1.5.0/bin/javaws

● Save it to disk

□ Always perform this action when handling files of this type

3. **In the Opening Jnlpgenerator-cli dialog, select** `Save it to disk`, **then click** `OK`**.**

   The Save As dialog appears.

4. **In the Save As dialog, specify the location where you want to save the** `jnlpgenerator-cli` **file.**

5. **Open the** `jnlpgenerator-cli` **file using a text editor and modify the port number referenced in this file.**

   For example:

```
<application-desc>

<argument>cli</argument>

<argument>2121</argument>

</application-desc>
```

In the `<application-desc>` you can change the **second argument** to any port number that you want to use.

6. **Save the changes you made and close the** `jnlpgenerator-cli` **file.**

7. **Use the** `javaws` **to start the Storage Redirection service from your local client.**

   For example:

```
javaws jnlpgenerator-cli
```

Note – If you do not use the default port number provided, you must always identify the non-default port number in the Storage Redirection command-line interface when starting, stopping or viewing storage redirections.

Securing the ILOM Remote Console

Topics

Description	Links	Platform Feature Support
Before you begin	• "Before You Begin" on page 192	• x86 system server SP • SPARC system server SP • CMM
Configure the ILOM Remote Console Lock option	• "Edit the ILOM Remote Console Lock Option" on page 192	

Before You Begin

Prior to configuring the ILOM Remote Console Lock option, the following prerequisites must be met:

- To enable the ILOM Remote Console Lock option in ILOM, you must have Console (c) role privileges associated with your user account.
- You must be running ILOM 3.0.4 or later on the server SP.

▼ Edit the ILOM Remote Console Lock Option

1. **Log in to the ILOM SP CLI or the CMM CLI.**

Note – When logging in to the CMM CLI, navigate to the SP target where you want to enable or disable the KVMS lock option for the ILOM Remote Console.

---

2. **To view all the possible properties associated with the management of the SP KVMS services, type:**

```
-> help /SP/services/kvms
```

The following sample output appears:

```
/SP/services/kvms : Management of the KVMS service
    Targets:

    Properties:
        custom_lock_key : KVMS custom lock key
        custom_lock_key : Possible values = esc, end, tab, ins,
del, home, enter, space, break, backspace, pg_up, pg_down,
scrl_lck, sys_rq, num_plus, num_minus, f1, f2, f3, f4, f5, f6, f7,
f8, f9, f10, f11, f12, a-z, 0-9, !, @, #, $, %, ^, &, *, (, ), -,
_, =, +,, |, ~, `, [, {, ], }, ;, :, ’, ", <, ., >, /, ?
        custom_lock_key : User role required for set = c

        custom_lock_modifiers : KVMS custom lock modifiers
        custom_lock_modifiers : Possible values = l_alt, r_alt,
l_shift, r_shift, l_ctrl, r_ctrl, l_gui, r_gui
        custom_lock_modifiers : User role required for set = c

        lockmode : KVMS lock mode
        lockmode : Possible values = disabled, windows, custom
        lockmode : User role required for set = c

        mousemode : KVMS mouse mode
        mousemode : Possible values = absolute, relative
        mousemode : User role required for set = c

        servicestate : KVMS service state
        servicestate : Possible values = enabled, disabled
        servicestate : User role required for set = a
```

3. **Perform any of the following tasks using either the `cd`, `set`, or `show` commands to manage the SP KVMS target properties.**

Task	Instructions
Navigate to the KVMS target.	• To navigate to the KVMS target, type the following command: -> **`cd /SP/services/kvms`** **Note -** You must navigate to the KVMS target prior to enabling or disabling the KVMS lock mode options.
Display the KVMS lock mode properties.	• To display the KVMS lock mode properties, type the following command: -> **`show`** The target, properties, and commands that are associated with the management of the SP KVMS service appear.
Disable the ILOM Remote Console lock mode feature.	• To disable the ILOM Remote Console lock mode feature, type the following command: **-> `set lockmode=disabled`**
Enable the standard Windows host lock mode feature.	• To enable the standard lock mode feature on a Windows system, type the following command: -> **`set lockmode=windows`**
Enable the custom host lock mode feature.	• To enable the custom lock mode feature on a Linux, Solaris, or Windows system, type following commands: -> **`set lockmode=custom`** -> **`set custom_lock_key=`**<*specify a custom lock key*> -> **`set lock_modifiers`**=<*specify up to four custom lock modifiers*> **Note -** Each custom lock modifier specified must be separated by a comma.

Enabled Custom Lock Mode Example

In this example, you have defined, in your host OS, the following custom keyboard shortcut sequence to log you off the operating system:

```
<shift><control><backspace>
```

To implement the above custom keyboard shortcut sequence while exiting an ILOM Remote Console session, the following KVMS properties would be set in the ILOM CLI:

```
/SP/services/kvms
    Targets:

    Properties:
        custom_lock_key = backspace
        custom_lock_modifiers = l_shift, l_ctrl
        lockmode = custom
        mousemode = absolute
        servicestate = enabled
```

CHAPTER 13

Managing Remote Host Power States, BIOS Boot Device, and Host Server Console

Topics

Description	Links
Control the power state of a remote server module	• "Issuing Remote Power State Commands for Host Server or CMM" on page 198
Remote Host Control - Boot Device on x86 system SP	• "Managing BIOS Boot Device on x86 Hosts" on page 200
Learn how to start the Host Console, change the display properties, as well as view the console history or bootlog.	• "Managing the Host Console" on page 203

Related Topics

For ILOM	Chapter or Section	Guide
• Concepts	• Remote Host Management Options	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide* (820-6410)
• Web interface	• Managing Remote Hosts Power States	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* (820-6411)
The ILOM 3.0 Documentation Collection is available at: `http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic`.		

Issuing Remote Power State Commands for Host Server or CMM

Topics

Description	Links	Platform Feature Support
Manage remote power control of host server	• "Issue Remote Power State Commands From Server SP or CMM CLI" on page 198	• x86 system server SP • SPARC system server SP • CMM

Issue Remote Power State Commands From Server SP or CMM CLI

From a command window or terminal, you can issue the following commands that are described in TABLE 13-1 and TABLE 13-2 to remotely control the power state of a host server or CMM.

TABLE 13-1 Server SP Remote Power State Commands

Power State Command	Description	Command Syntax Example
`start`	Use the `start` command to turn on full power to the remote host server. To issue the `start` command:	
	• From the server SP CLI, type:	`start /SYS`
	• From CMM CLI for a blade server with a single dedicated SP, type:	`start /CH/BLn/SYS`
	• From CMM CLI for a blade server with two dedicated SPs, type:	`start /CH/BLn/NODEn/SYS`
`stop`	Use the `stop` command to shut down the OS gracefully prior to powering off the host server. To issue the `stop` command:	
	• From the server SP CLI:	`stop /SYS`
	• Form the CMM CLI for a blade server with a single dedicated SP:	`stop /CH/BLn/SYS`

TABLE 13-1 Server SP Remote Power State Commands *(Continued)*

Power State Command	Description	Command Syntax Example
	• For blade server with two dedicated SPs:	`stop /CH/BLn/NODEn/SYS`
`stop -force`	Use the `stop -force` command to immediately turn off the power to the remote host server. To issue the `stop -force` command:	
	• From the server SP CLI, type:	`stop -force /SYS`
	• From CMM CLI for blade server with single dedicated SP, type:	`stop -force /CH/BLn/SYS`
	• From CMM CLI for a blade server with two dedicated SPs, type:	`stop -force /CH/BLn/NODEn/SYS`
`reset`	Use the `reset` command `to immediately` reboot the remote host server. To issue the `reset` command:	
	• From the server SP CLI, type:	`reset /SYS`
	• From CMM CLI for a blade server with single a dedicated SP, type:	`reset /CH/BLn/SYS`
	• From CMM CLI for a blade server with two dedicated SPs, type:	`reset /CH/BLn/NODEn/SYS`

TABLE 13-2 Chassis Monitoring Module (CMM) Remote Power State Commands

Power State Command	Description	Command Syntax Example
`start`	Use the `start` command to turn on full power to the remote chassis. To issue the `start` command to the remote chassis from the CMM CLI, type	`start /CH`
stop	Use the stop command to shut down the power on the chassis and its components gracefully. To issue the `stop` command to the remote chassis from the CMM CLI, type:	`stop /CH`
`stop -force`	Use the `stop -force` command to immediately turn off the power to the chassis and its components. To issue the `stop -force` command to the remote chassis from the CMM CLI, type:	`stop -force /CH`

For information about connecting to a host server or issuing commands from the ILOM CLI, see "Configuring ILOM Communication Settings" on page 29.

Managing BIOS Boot Device on x86 Hosts

Topics

Description	Links	Platform Feature Support
Review the prerequisites	• "Before You Begin" on page 201	• x86 system server SP
Control BIOS boot device order	• "Configure BIOS Host Boot Device Override" on page 201	

Before You Begin

- The Reset and Host Control (`r`) role is required to change the host boot device configuration variable.

Note – The Host Control BIOS boot device feature is supported on x86 system SPs. This feature is not supported on the CMM or on SPARC system SPs. For information about ILOM Host Control boot options on SPARC systems, consult the online ILOM Supplement guide or platform Administration guide provided for that system.

Follow the steps in the following procedure to override the BIOS boot device setting from ILOM by using the Host Control features.

▼ Configure BIOS Host Boot Device Override

1. **Log in to the ILOM SP CLI.**
2. **Use the `cd` and `show` commands to navigate to the host system.**

   For example:

```
->cd /HOST
/HOST

->show

/HOST
   Targets:
       diag

   Properties:
       boot_device = default
       generate_host_nmi = (Cannot show property)

   Commands:
       cd
       set
       show
```

3. **To set the host boot device for the next time the system is powered on, type:**

   `->`**`set boot_device=`***value*

   Possible values are:

- `default` – Setting the value to `default` means that there is no override to the BIOS settings. Setting to `default` will also clear any previously chosen selection.
- `pxe` – Setting the value to `pxe` means that at the next host boot, the BIOS boot order settings will be temporarily bypassed and instead the host will boot from the network, following the PXE boot specification.
- `disk` – Setting the value to `disk` means that at the next host boot, the BIOS boot order settings will be temporarily bypassed and instead the host will boot from the first disk as determined by BIOS. The specific disk chosen depends on configuration. Typically, hosts use this option by default and the host's behavior might not change by selecting this option.
- `diagnostic` – Setting the value to `diagnostic` means that at the next host boot, the BIOS boot order settings will be temporarily bypassed and instead the host will boot into the diagnostic partition, if configured.
- `cdrom` – Setting the value to `cdrom` means that at the next host boot, the BIOS boot order settings will be temporarily bypassed and instead the host will boot from the attached CD-ROM or DVD device.
- `bios` – Setting the value to `bios` means that at the next host boot, the BIOS boot order settings will be temporarily bypassed and instead the host will boot into the BIOS Setup screen.

Managing the Host Console

Topics

Description	Links	Platform Feature Support
Review the prerequisites	• "Before You Begin" on page 203	• x86 system server SP • SPARC server
View and set Host Console properties	• "View and Configure Host Console Properties" on page 203	
Start Host Console and view Console History or Bootlog History	• "Start Host Console and Display Console History and Bootlog" on page 206	

Before You Begin

- To change the Host Console properties, you must have the Admin (a)role enabled.
- As of ILOM 3.0.12, Host Console properties (`line_count`, `pause_count` and `start_from`) are no longer persistent across all sessions. The values for these properties are valid only for the length of that particular spsh session.

▼ View and Configure Host Console Properties

1. Log in to the ILOM SP CLI.

2. **Use the** `cd` **and** `ls` **commands to navigate to the host console properties.**

   For example:

```
-> cd /HOST/console
/HOST/console

-> ls

 /HOST/console
    Targets:
        history

    Properties:
        escapechars = #.
        line_count = 0
        pause_count = 0
        start_from = end

    Commands:
        cd
        show
        start
        stop
```

Note – Each time an spsh session is started, it initializes these properties to their default values: `line_count` = `0`, `pause_count` = `0`, `start_from` = `end`. The values for these properties are valid only for the length of that particular spsh session.

3. **Use the `help` command to view descriptions about the Host Control proeprties.**

   For example:

```
-> help escapechars
    Properties:
       escapechars : set escape chars using the console connection
        escapechars : User role required for set = a

-> help line_count
    Properties:
        line_count : total number of lines to display
       line_count : Possible values = 0-2048 where 0 means no limit
        line_count : User role required for set = c

-> help pause_count
    Properties:
       pause_count : number of lines to display before each pause
      pause_count : Possible values = 0-2048 where 0 means no limit
        pause_count : User role required for set = c

-> help start_from
    Properties:
       start_from : from which end of the available history to list
        start_from : Possible values = beginning,end
        start_from : User role required for set = c
```

4. **Use the `set` command to configure the Host Console properties.**

   For example:

   - To set a value for the `line_ count` property, type

     -> **`set line_count=`***value*

     Where *value* can range from 1 to 2048 lines.

   - To set a value for the `pause_count` property, type:

     -> **`set pause_count=`***value*

     Where *value* can range from 1 to any valid integer or for infinite number of lines. The default is not to pause.

   - To set a value for the `start_from` property, type:

     -> **`set start_from=`***value*

     Where the *value* can equal *end* or *beginning*. The *end* value is the last line (most recent) in the buffer (the default). The *beginning* value is the first line in the buffer.

   - To set a value for `escapechars`, type:

     -> **`set escapechars=`***value*

Where the *value* is limited to two characters. The default value is `#.` (Hash-Period).

Note – The `/SP/console` `escapechars` property enables you to specify an escape character sequence to use when switching from a system console session back to ILOM. Changing the escape character does not take effect in a currently active console session.

▼ Start Host Console and Display Console History and Bootlog

1. **Log in to the ILOM SP CLI.**
2. **Set the Host Console display properties, see** "View and Configure Host Console Properties" on page 203**.**

Note – As of ILOM 3.0.12, Host Console properties (`line_count`, `pause_count` and `start_from`) are no longer persistent across all sessions. The values for these properties are valid only for the length of that particular spsh session.

---

3. **To start the host console, type:**

   ```
   ->start /SP/console
   ```

4. **To display the Console History, type:**

   ```
   -> show /SP/console/history
   ```

   The Console History buffer is a circular buffer that can contain up to 1 Mbyte of information. The buffer captures all POST and boot information as well as any OS information that is controlled through the Host Console.

5. **To display the Bootlog type:**

   ```
   ->show /SP/console/bootlog
   ```

   The Bootlog tracks the systems's start-up progress and logs any problems that might occur.

CHAPTER 14

Managing TPM and LDom States on SPARC Servers

Topics

Description	Links
Control the TPM state on a SPARC server	• "Controlling the TPM State on a SPARC Server" on page 208
Manage Logical Domain (LDom) configurations on SPARC servers	• "Managing LDom Configurations on SPARC Servers" on page 211

Related Topics

For ILOM	Chapter or Section	Guide
• Concepts	• Remote Host Management Options	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide* (820-6410)
• Web interface	• Managing TPM and LDom States on SPARC Servers	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* (820-6411)

The ILOM 3.0 Documentation Collection is available at: `http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic`.

Controlling the TPM State on a SPARC Server

Topics

Description	Links	Platform Feature Support
Review the prerequisites	• "Before You Begin" on page 208	• SPARC system SP
Control the TPM state on a SPARC server.	• "Control TPM State on a SPARC Server" on page 208	

Before You Begin

- The Trusted Platform Module (TPM) feature in ILOM is available for SPARC servers only.
- The SPARC server should be running a version of the Oracle Solaris operating system that supports TPM.

  For more information about configuring TPM support in Solaris, see the Solaris documentation or the platform documentation shipped with your server.
- You must be using ILOM 3.0.8 or a later version on the SPARC server SP.
- You need to have the Reset and Host Control (`r`) user account to modify the TPM settings in ILOM.

▼ Control TPM State on a SPARC Server

1. **Log in to the ILOM SP CLI.**
2. **Use the `show` command to display the TPM target, properties, and commands.**

   For example:

```
-> show /HOST/tpm

/HOST/tpm
    Targets:

    Properties:
        activate = false
        enable = false
        forceclear = false

    Commands:
        cd
        set
        show

->
```

3. **Use the** `help` **command to view details about the TPM target and properties.**

   For example:

```
-> help /HOST/tpm

/HOST/tpm : Host TPM (Trusted Platform Module) Knobs
    Targets:

    Properties:
       activate : TPM Activate Property. If set to TRUE, then TPM
will be activated if the 'enable' property is also set to TRUE.
        activate : Possible values = true, false
        activate : User role required for set = r

        enable : TPM Enable Property. If not enabled, then TPM
configuration changes can not be made.
        enable : Possible values = true, false
        enable : User role required for set = r

       forceclear : TPM Forceclear Property. If set to TRUE, then
TPM state will be purged on the next power on event if and only if
the 'enable' property is set to TRUE.
        forceclear : Possible values = true, false
        forceclear : User role required for set = r
```

4. **Use the** `set` **command to specify the TPM property values**.

   For example:

- set command usage:

  ```
  set [target] <property>=<value> [<property>=<value>]
  ```

- At the prompt, you would type the TPM target and one or more property values as follows:

  -> **set /host/tpm** *property*=*value*

  -> **set /host/tpm** *property*=*value* *property*=*value*

Where *property* and *value* can be any of the following parameters specified in the following table:

Property	Values	Example
`enable`	Accepts `true` or `false`. **Note -** The default value for `enable` is `false`.	To enable the TPM state, you would type: -> **`set /HOST/tpm enable=true`** **Note -** To apply the enabled TPM state on the SPARC server the next time the server powers on, you must activate it. For more details, see `activate` property.
`activate`	Accepts `true` or `false`. **Note -** The default value for `activate` is `false`.	To enable the TPM state and activate this enabled state on the SPARC server the next time the server powers on, you would type: **`-> set /HOST/tpm enable=true activate=true`**
`forceclear`	Accepts `true` or `false`. **Note -** The default value for `forceclear` is `false`.	To purge (disable) an enabled TPM state on the SPARC server the next time the server powers on, you would type: -> **`set /HOST/tpm forceclear=true`** **Note -** `forceclear` will only set to `true`, if `enable` and `activate` are also set to `true`.

Managing LDom Configurations on SPARC Servers

Topics

Description	Links	Platform Feature Support
Review the prerequisites	• "Before You Begin" on page 211	• SPARC system SP
View and manage ILOM settings for stored LDom configurations.	• "View Targets and Properties for Stored LDom Configurations on SPARC T3 Series Server" on page 212 • "Specify Host Power to a Stored LDom Configuration" on page 213 • "Enable or Disable the Control Domain Property Values" on page 213	

Before You Begin

To view and manage the ILOM settings for stored Logical Domain (LDom) configurations, the following requirements must be met:

- You must access ILOM on a SPARC server that has the appropriate ILOM point release firmware installed (see Note below).

Note – ILOM 3.0.12 or later is required to view the LDom targets and properties from a SPARC T3 Series server. ILOM 2.0.0 or later is required to: (1) specify which LDom configuration is used on the host SPARC server, and (2) to manage the boot property values for the control domain from the host SPARC server.

- You must have the Oracle VM Server for SPARC (Logical Domains Manager) 2.0 or later software installed on your host SPARC server.
- The host SPARC server must have saved LDom configurations. For instructions on how to create and save LDom configurations on a host SPARC server, see the *Logical Domains 1.3 Administration Guide* (821-0406).
- You must have Remote Host Reset and Host Control (r) privileges in ILOM to set the:

- LDom `bootmode` target
- `The bootmode` property values for the primary or guests domain

▼ View Targets and Properties for Stored LDom Configurations on SPARC T3 Series Server

To view the CLI targets and properties for saved LDom configurations on SPARC T3 Series server, follow these steps:

1. **Log in to the ILOM CLI on a SPARC T3 Series server.**
2. **To view the names of saved LDom host configurations, type:**

   -> **`show /HOST/domain/configs`**

3. **To view the property values for the creation date of the saved LDom configuration and the number of domains configured in the saved LDom configuration, you would type:**

   -> **`show /HOST/domain/configs/`**<*name_of_stored_ configuration*>

   For example, the following example shows a sample CLI output for viewing the property values associated with a fictitious stored LDom configuration named `ONEDOMAIN`.

```
-> show
/HOST/domain/configs
    Targets:
        trimmed
        ONEDOMAIN
Properties:

    Commands:
        cd
        show

-> show ONEDOMAIN
/HOST/domain/configs/ONEDOMAIN
    Targets:
Properties:
        date_created = 2010-08-17 17:09:34
        domains = 1

    Commands:
        cd
        show
```

Note – ILOM stores the read-only properties in non-volatile memory and updates them each time an LDom configuration in LDom Manager is updated

Specify Host Power to a Stored LDom Configuration

To specify which stored LDom configuration is used when the host server is powered-on, follow these steps:

1. **Log in to the ILOM CLI on a SPARC server.**
2. **Use the** `cd` **command to navigate to the** `/Host/bootmode` **target, then use the** `set config=` **command to specify the name of the stored LDom configuration.**

   For example:

   The following example shows a sample CLI output for setting a fictitious stored LDom configuration named `ONEDOMAIN` as the `bootmode` target.

```
-> cd /HOST/bootmode
/HOST/bootmode

-> set config=ONEDOMAIN
Set 'config' to 'ONEDOMAIN'
```

   Note that changes made to the LDom configuration `bootmode` properties will take effect on the next host server reset or power-on.

Enable or Disable the Control Domain Property Values

To enable or disable the LDom Control Domain boot property values in ILOM, follow these steps:

1. **Log in to the ILOM CLI on a SPARC server.**
2. **Use the** `cd` **command to navigate to the** `/Host/domain/control` **target, then use the** `ls` **command to view the auto-boot properties for the host control domain and guest domains**.

   For example:

```
-> cd /HOST/domain/control
-> ls

 /HOST/domain/control
    Targets:

    Properties:
        auto-boot = enabled
        boot_guests = enabled

    Commands:
        cd
        reset
        set
        show
```

3. **Use the `set` command to specify the following `auto-boot` and `boot-guests` property values:**

Property	Set Property Value	Description
`auto-boot`	`set auto-boot=<`*value*`>`	Type the `set auto-boot=` command followed by one of the following property values: • `enabled` (default). Enabling the `auto-boot` property value will automatically reboot the control domain after the next power-on or reset. • `disabled`. Disabling the `auto-boot` property value on the control domain will prevent automatic reboots and stop the control domain at the OpenBoot `ok` prompt after the next power-on or reset.
`boot_guests`	`set boot_guests=<`*value*`>`	Type the `set boot_guests=` command followed by one of the following property values: • `enabled` (default). Enabling the `boot_guests` property enables the guest domain to boot after the next power-on or reset. • `disabled`. Disabling the `boot_guests` property value for the guest domains will prevent the guest domains from booting after the next power-on or reset.

CHAPTER 15

Performing Remote Host System Diagnostics

Topics

Description	**Links**
Diagnose x86 system hardware issues	• "Diagnosing x86 Systems Hardware Issues" on page 216
Diagnose SPARC system hardware issues	• "Diagnosing SPARC Systems Hardware Issues" on page 218
Collect data for use by Oracle Services personnel to diagnose system problems	• "Collecting SP Data to Diagnose System Problems" on page 222

Related Topics

For ILOM	**Chapter or Section**	**Guide**
• Concepts	• Diagnostics for x86 or SPARC Systems • Collect SP Data to Diagnose System Problems	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide* (820-6410)
• Web interface	• Diagnostics • Collect SP Data to Diagnose System Problems	*Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* (820-6411)

The ILOM 3.0 Documentation Collection is available at: `http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic`.

Diagnosing x86 Systems Hardware Issues

Topics

Description	Links	Platform Feature Support
Review the prerequisites	• "Before You Begin" on page 219	• x86 system server SP
Ensure that the requirements for configuring and running diagnostic tests are met	• "Configure and Run Pc-Check Diagnostics" on page 216	
Configure and run Pc-Check diagnostic tests	• "Configure and Run Pc-Check Diagnostics" on page 216	
Generate a NMI to a host	• "Generate a Non-Maskable Interrupt" on page 217	
Run other x86 system hardware diagnostic tests and tools	• *Sun x64 Servers Diagnostics Guide* (820-6750)	

Before You Begin

- To diagnose x86 systems hardware issues, you need the Reset and Host Control (`r`) role enabled.

▼ Configure and Run Pc-Check Diagnostics

1. **Log in to the ILOM SP CLI.**
2. **Type the following commands to enable the diagnostic tests:**

```
-> cd /HOST/diag/
/HOST/diag

-> show /HOST/diag
   Targets:

   Properties:
     state = disabled

   Commands:
       cd
       set
       show

-> set state=extended This will enable Pc-Check to run a 20-40 minute test suite
OR
-> set state=enabled    This will enable Pc-Check to run a 4-5 minute test suite
OR
-> set state=manual    This will enable you to select specific Pc-Check tests to run

-> show
   Targets:

   Properties:
       state = enabled

   Commands:
       cd
       set
       show
```

3. **Reset the power on the host to run the PC diagnostic tests.**

▼ Generate a Non-Maskable Interrupt

Caution – Depending on the host OS configuration, generating a non-maskable interrupt (NMI) might cause the OS to crash, stop responding, or wait for external debugger input.

---

1. **Log in to the ILOM SP CLI.**

2. **Type the following commands:**

```
-> cd /HOST
/HOST

-> show
/HOST
Targets:
     diag

Properties:
     generate_host_nmi = (Cannot show property)

Commands:
     cd
     set
     show

-> set generate_host_nmi=true
set 'generate_host_nmi' to 'true'
```

Diagnosing SPARC Systems Hardware Issues

Topics

Description	Links	Platform Feature Support
Review the prerequisites	• "Before You Begin" on page 219	• SPARC system server SP
Configure the system to run diagnostic tests	• "Configure Diagnostics Mode" on page 219	
Specify which diagnostic triggers to activate	• "Specify the Diagnostics Trigger" on page 219	
Specify the level of diagnostics that you want to execute	• "Specify Level of Diagnostics" on page 220	
Specify the verbosity output of the executed diagnostic tests	• "Specify Verbosity of Diagnostics Output" on page 221	

Before You Begin

Prior to performing the procedures in this section, the following requirement must be met:

- To configure and run diagnostic tests on a SPARC system, you need the Reset and Host Control (r) role enabled.

▼ Configure Diagnostics Mode

Use the /HOST/diag host mode property to control whether diagnostics are enabled and to specify which diagnostic mode is enabled.

Follow these steps to configure the diagnostic mode:

1. **Log in to the ILOM SP CLI.**

2. **At the command prompt, type the following command:**

   ```
   -> set /HOST/diag mode=value
   ```

   Where *value* is one of the following:

   - off – Do not run any diagnostics.
   - normal – Run diagnostics (the default value).

3. **Reset the power on the host to run the diagnostic tests.**

▼ Specify the Diagnostics Trigger

You can select one or more triggers that will cause a power-on self-test (POST) to be run on the host.

Follow these steps to set the trigger levels:

1. **Log in to the ILOM SP CLI.**

2. **At the command prompt, type the following command**

   ```
   -> set /HOST/diag trigger=value
   ```

   Where *value* can be one of the following:

   - none – Diagnostics will not be triggered to run.
   - user-reset – Diagnostics will be run upon a user-invoked reset.
   - power-on-reset – Diagnostics will be run when power is applied.
   - error-reset – Diagnostics will be run upon any error-invoked reset.
   - all-resets – Diagnostics will be run for any of the above reset types.

▼ Specify Level of Diagnostics

There are separate ILOM CLI properties that enable you to specify the level of diagnostic testing to be executed, depending on how the diagnostics were triggered to run. This gives granular control of how much diagnostic testing is performed in different host reset situations.

Use the `/HOST/diag` *level* property to specify the level of diagnostic testing to be executed when diagnostics are enabled.

Follow these steps to specify the level of diagnostics to be executed:

1. **Log in to the ILOM SP CLI.**

2. **Perform the one of the following commands, depending on how the host is reset:**

   - To specify the diagnostic level when the host is powered on, type the following command:

     ```
     > set /HOST/diag power_on_level=value
     ```

   - To specify the diagnostic level when the host is reset by the user, type the following command:

     ```
     -> set /HOST/diag user_reset_level=value
     ```

   - To specify the diagnostic level when the host is reset due to a system error, type the following command:

     ```
     -> set /HOST/diag error_reset_level=value
     ```

   Where *value* is one of the following:

   - `min` – Run the minimum level of diagnostics to verify the system.
   - `max` – Run the maximum set of diagnostics to fully verify system health (the default value).

Note – For backward compatibility with ILOM 2.x, the former property `/HOST/diag` *level* is still supported as a shortcut for specifying the same diagnostic level for all trigger types. Any value set to `/HOST/diag` *level* will be applied to all three trigger-specific properties: `power_on_level`, `user_reset_level`, and `error_reset_level`.

---

3. **Reset the power on the host to run the diagnostic tests.**

▼ Specify Verbosity of Diagnostics Output

There are specific ILOM CLI properties that enable you to specify the output verbosity of executed diagnostics, depending on how the diagnostics were triggered to run. This gives granular control of how much diagnostics output is given in different host reset situations.

Follow these steps to specify the verbosity of the diagnostics output:

1. **Log in to the ILOM SP CLI.**

2. **Perform one of the following commands, depending on how the host was reset:**

   - To specify the output verbosity for diagnostics executed when the host is powered on, type the following command:

     ```
     > set /HOST/diag power_on_verbosity=value
     ```

   - To specify the output verbosity for diagnostics executed when the host is reset by the user, type the following command:

     ```
     -> set /HOST/diag user_reset_verbosity=value
     ```

   - To specify the output verbosity for diagnostics executed when the host is reset due to a system error, type the following command:

     ```
     -> set /HOST/diag error_reset_verbosity=value
     ```

   Where *value* is one of the following:

   - `none` – Diagnostics do not print any output on the system console when running, unless a fault is detected.
   - `min` – Diagnostics print a limited amount of output on the system console.
   - `normal` – Diagnostics print a moderate amount of output on the system console (the default value).
   - `max` – Diagnostics print full output on the system console, including the name and results of each test being run.
   - `debug` – Diagnostics print extensive debugging output on the system console, including devices being tested and debug output of each test.

Note – For backward compatibility with ILOM 2.x, the former property `/HOST/diag` *verbosity* is still supported as a shortcut for specifying the same output verbosity for all trigger types. Any value set to `/HOST/diag` *verbosity* will be applied to all three trigger-specific verbosity properties: `power_on_verbosity`, `user_reset_verbosity`, and `error_reset_verbosity`.

---

3. **Reset the power on the host to run the diagnostic tests.**

Collecting SP Data to Diagnose System Problems

Topics

Description	Links	Platform Feature Support
Review the prerequisites	• "Before You Begin" on page 222	• Oracle Service personnel feature only
Collect SP data	• "Collect SP Data to Diagnose System Problems" on page 222	

Before You Begin

- To collect SP data using the Service Snapshot utility, you need the Admin (a) role enabled.

⚠ **Caution –** The purpose of the ILOM Service Snapshot utility is to collect data for use by Oracle Services personnel to diagnose problems. Customers should not run this utility unless requested to do so by Oracle Services.

▼ Collect SP Data to Diagnose System Problems

Follow these steps to run the Service Snapshot utility:

1. **Log in to the ILOM SP CLI.**

2. **Type the following commands:**

```
->set /SP/diag/snapshot dataset=data
->set /SP/diag/snapshot dump_uri=URI
```

Where *data* and *URI* are one of the following:

Variable	Option	Description
data	`normal`	Specifies that ILOM, operating system, and hardware information is to be collected.
	`FRUID`	Available as of ILOM 3.0.3, requests ILOM to collect information about FRUs currently configured on your server in addition to the data collected by the `normal` option.
	`full`	Specifies that all data is to be collected ("full" collection). **Note -** Using this option might reset the running host.
	• `normal-logonly` • `fruid-logonly` • `full-logonly`	Specifies that only log files are to be collected.

URI	Any valid target directory location	Specifies the URI of the target directory. The URI format is as follows:
		`protocol://username:password@host/directory`
		Where protocol can be one of these transfer methods: SFTP or FTP.
		For example, to store the snapshot information in the directory named `data` on the host, define the *URI* as follows:
		`ftp://joe:`*mypasswd@host_ip_address*`/data`
		The directory `data` is relative to the user's login, so the directory would probably be `/home/joe/data`.

APPENDIX **A**

CLI Command Reference

CLI Command Reference

This appendix contains the most common ILOM commands used to administer your Oracle Sun server from the ILOM command-line interface (CLI).

Syntax examples in this appendix use the target starting with `/SP/`which applies to most Oracle Sun servers. However, if you are performing these commands from a CMM, you can interchange the starting `/SP/` target with `/CMM/` since the sub-targets are common across all server platforms. Or, if you are performing these commands from a server blade in a chassis monitoring module (CMM), you can the interchange the starting `/SP/` target with `/CH/BL`*n* or `CH/BL`*n*`/Node`*n* depending the server blade platform.

`cd` Command

Use the `cd` command to navigate the namespace. When you `cd` to a target location, that location then becomes the default target for all other commands. Using the `-default` option with no target returns you to the top of the namespace. Typing `cd -default` is the equivalent of typing `cd /`. Typing just `cd` displays your current location in the namespace. Typing `help targets` displays a list of all targets in the entire namespace.

Syntax

`cd` *target*

Options

[-default] [-h|help]

Targets and Properties

Any location in the namespace.

Examples

To create a user named `emmett`, **`cd`** to `/SP/users`, then execute the create command with `/SP/users` as the default target.

```
-> cd /SP/users
```

```
-> create emmett
```

To find your location, type **`cd`**.

```
-> cd /SP/users
```

`create` Command

Use the `create` command to set up an object in the namespace. Unless you specify properties with the `create` command, they are empty.

Syntax

create [*options***]** *target* **[***propertyname=value***]**

Options

[-h|help]

Targets, Properties, and Values

TABLE A-1 Targets, Properties and Values for `create` Command

Valid Targets	Properties	Values	Default
/SP/users/*username*	password role	<string> administrator | operator | a | u | c | r | o | s	(none) o
/SP/services/snmp/communities /*communityname*	permissions	ro | rw	ro
/SP/services/snmp/user/ *username*	authenticationprotocol authenticationpassword permissions privacyprotocol privacypassword	MD5 <string> ro | rw none | DES <string>	MD5 (null string) ro DES (null string)

Example

```
-> create /SP/users/susan role=administrator
```

`delete` Command

Use the `delete` command to remove an object from the namespace. You will be prompted to confirm a `delete` command. Eliminate this prompt by using the `-script` option.

Syntax

delete [*options***] [-script]** *target*

Options

[-h|help] [-script]

Targets

TABLE A-2 Targets for `delete` Command

Valid Targets
/SP/users/*username*
/SP/services/snmp/communities/*communityname*
/SP/services/snmp/user/*username*

Examples

```
-> delete /SP/users/susan
```

```
-> delete /SP/services/snmp/communities/public
```

`dump` Command

Use the `dump` command to transfer a file from a target to a remote location specified by the URI.

Syntax

dump -destination <*URI***>** *target*

Options

[-destination]

`exit` Command

Use the `exit` command to end a CLI session.

Syntax

exit [*options***]**

Options

[-h|help]

`help` Command

Use the `help` command to display Help information about commands and targets. Using the `-o|output terse` option displays usage information only. The `-o|output verbose` option displays usage, description, and additional information including examples of command usage. If you do not use the `-o|output` option, usage information and a brief description of the command are displayed.

Specifying *command targets* displays a complete list of valid targets for that command from the fixed targets in `/SP` and `/SYS`. Fixed targets are targets that cannot be created by a user.

Specifying the `legal` command target displays the copyright information and product use rights.

Syntax

help [*options***]** *command target*

Options

[-h|help] [-o|output terse|verbose]

Commands

cd, create, delete, exit, help, load, reset, set, show, start, stop, version

Examples

```
-> help load
The load command transfers a file from a remote location specified
by the URI and updates the given target.
Usage: load [-script] -source <URI> [target]
-source: Specify the location to get a file.
```

```
-> help -output verbose reset
The reset command is used to reset a target.
Usage: reset [-script] [target]
Available options for this command:
-script: Do not prompt for yes/no confirmation and act as if yes
were specified.
```

`load` Command

Use the `load` command to transfer an image file from a source, indicated by a Uniform Resource Indicator (URI), to update ILOM firmware. The URI can specify a protocol and credentials used for the transfer. The `load` command supports multiple protocols (TFTP, SCP, FTP). If credentials are required and not specified, the command prompts you for a password. Using the `-script` option eliminates the prompt for a yes or no confirmation and the command acts as if yes were specified.

Note – Use this command to update your ILOM firmware and BIOS.

TABLE A-3 Targets, Properties, and Values for `load` Command

Valid Targets	Properties	Values	Default
/SP/users/*username*	password	<string>	(none)
	role	administrator|operator |a|u|c|r|o|s	o

Syntax

load -source *URI*

Options

[-h|help] [-script]

Example

```
 -> load -source tftp://ip_address/newmainimage
```

Note – A firmware upgrade will cause the server and ILOM to be reset. It is recommended that a graceful shutdown of the server be done prior to the upgrade procedure. An upgrade takes about five minutes to complete. ILOM will enter a special mode to load new firmware. No other tasks can be performed in ILOM until the firmware upgrade is complete and ILOM is reset.

```
 -> load -source tftp://ip_address/newmainimage
Are you sure you want to load the specified file (y/n)? y
File upload is complete.
Firmware image verification is complete.
Do you want to preserve the configuration (y/n)? n
Updating firmware in flash RAM:
.
Firmware update is complete.
ILOM will not be restarted with the new firmware.
```

`reset` Command

Use the `reset` command to reset the state of the target. You will be prompted to confirm a reset operation. Eliminate this prompt by using the `-script` option.

Note – The `reset` command does not affect the power state of hardware devices.

Syntax

`reset` **`[`***options***`]`** *target*

Options

`[-h|help] [-script]`

(The `-f|force` option is supported on SPARC-based systems.)

Targets

TABLE A-4 Targets for `reset` Command

Valid Targets
/SP
/SYS

Examples

```
-> reset /SP
```

```
-> reset /SYS
```

`set` Command

Use the `set` command to specify the properties of the target.

Syntax

set **[***options***]** *target* **[***propertyname***=***value***]**

Options

[-h|help]

Targets, Properties, and Values

TABLE A-5 Targets, Properties, and Values for `set` Command

Valid Targets	Properties	Values	Default
/HOST/tpm	enable	true | false	false
	activate	true | false	false
	forceclear	true | false	false
/SP/alertmgmt/rules	testalert	true	(none)
/SP/alertmgmt/rules/ *rulename* (*rulename* = 1 through 15)	community_or_username	<string>	public
	destination	email_address	(none)
	destination_port	<integer>	0
	event_class_filter	“ “ | Log | Email | Internal | Captive Shell | Backup | Restore | Audit | IPMI | Chassis | Fault | System | ActDir	(none)
	event_type_filter	“ “ | Developer | Connection | Send | Product | Chassis | Command Entered | State | Action | Fault | Repair | Warning	(none)
	level	disable | down | critical | major | minor	(none)
	snmp_version	1 | 2c | 3	3
	type	email | ipmipet | snmptrap	(none)
/SP/cli	timeout	<integer>	(none)
/SP/clock	datetime	current date and time	<*string*>
	timezone	EST | PST8PDT	GMT
	usentpserver	enabled | disabled	disabled
/SP/console/history	line_count	<integer>	0
	pause_count	<integer>	0
	start_from	end | beginning	end
/SP/services/http	port	<integer>	80
	secureredirect	enabled | disabled	enabled
	servicestate	enabled | disabled	disabled

TABLE A-5 Targets, Properties, and Values for `set` Command *(Continued)*

Valid Targets	Properties	Values	Default
/SP/services/https	port	<integer>	443
	servicestate	enabled | disabled	disabled
/SP/services/ipmi	servicestate	enabled | disabled	enabled
/SP/services/kvms	mousemode	absolute | relative	absolute
	servicestate	enabled | disabled	enabled
/SP/services/snmp	engineid	<hexadecimal>	*IP address*
	mibs	dump_uri	(none)
	port	<integer>	161
	sets	enabled | disabled	disabled
	v1	enabled | disabled	disabled
	v2c	enabled | disabled	disabled
	v3	enabled | disabled	enabled
	servicestate	enabled | disabled	enabled
/SP/services/snmp/ communities/private	permission	ro | rw	rw
/SP/services/snmp/ communities/public	permission	ro | rw	ro
/SP/services/snmp/user */username*	authenticationprotocol	MD5	MD5
	authenticationpassword	<string>	(null string)
	permissions	ro | rw	ro
	privacyprotocol	none | DES	DES
	privacypassword	<string>	(null string)
/SP/services/ssh	external_host		
	generate_new_key_action	true	(none)
	generate_new_key_type	rsa | dsa	(none)
	restart_sshd_action	true	(none)
	state	enabled | disabled	enabled
/SP/services/sso	state	enabled | disabled	enabled
/SP/users/*username*	role	administrator | operator | a | u | c | r | o | s	(none)
	password	<string>	(none)

TABLE A-5 Targets, Properties, and Values for `set` Command *(Continued)*

Valid Targets	Properties	Values	Default
`/SP/clients/activedirectory`	state	enabled | disabled	disabled
	defaultrole	administrator | operator | a| u | c| r | o | s	(none)
	dnslocatormode	enabled | disabled	disabled
	expsearchmode	enabled | disabled	disabled
	address	<ip address> or <DNS name>	(none)
	port	<integer between 0-65535>	0
	strictcertmode	enabled | disabled	disabled
	timeout	<integer>	4
	logdetail	none | high | medium | low | trace	none
`/SP/clients/activedirectory/admingroups/`*n* where *n* is 1-5	name	<string>	(none)
`/SP/clients/activedirectory/opergroups/`*n* where *n* is 1-5	name	<string>	(none)
`/SP/clients/activedirectory/userdomains/`*n* where *n* is 1-5	domain	<string>	(none)
`/SP/clients/activedirectory/customgroups/`*n* where *n* is 1-5	name	<string>	(none)
	roles	a|u|c|r|o|s|administrator| operator	o
`/SP/clients/activedirectory/alternateservers/`*n* where *n* is 1-5	address	<ip address> or <DNS name>	(none)
	port	<integer>	0

TABLE A-5 Targets, Properties, and Values for `set` Command *(Continued)*

Valid Targets	Properties	Values	Default
`/SP/clients/activedirectory/alternateservers/`*n*`/cert` where *n* is 1-5	certstatus	<string>	certificate not present
	clear_action	true	(none)
	issuer	<string>	(none)
	load_uri	tftp | ftp | scp	(none)
	serial_number	<string>	(none)
	subject	<string>	(none)
	valid_from	<string>	(none)
	valid_until	<string>	(none)
	version	<string>	(none)
`/SP/clients/activedirectory/cert/`	certstatus	<string>	certificate not present
	clear_action	true	(none)
	issuer	<string>	(none)
	load_uri	tftp | ftp | scp	(none)
	serial_number	<string>	(none)
	subject	<string>	(none)
	valid_from	<string>	(none)
	valid_until	<string>	(none)
	version	<string>	(none)
`/SP/clients/activedirectory/dnslocatorqueries/`*n* where *n* is 1-5	service	<DOMAIN>	(none)
`/SP/clients/dns`	auto_dns	enabled | disabled	disabled
	nameserver	<string>	(none)
	retries	<integer between 0 and 5>	(none)
	searchpath	<string>	(none)
	timeout	<integer between 1 and 10>	(none)
`/SP/clients/ldap`	binddn	<username>	(none)
	bindpw	<string>	(none)
	defaultrole	administrator | operator | a | u | c | r | o | s	o
	address	<ipaddress> | none	(none)
	port	<integer>	389
	searchbase	<string>	(none)
	state	enable | disabled	disabled

TABLE A-5 Targets, Properties, and Values for `set` Command *(Continued)*

Valid Targets	Properties	Values	Default
`/SP/clients/ldapssl`	state	enabled | disabled	disabled
	defaultrole	administrator | operator | a| u | c| r | o | s	(none)
	dnslocatormode	enabled | disabled	disabled
	address	<ip address> or <DNS name>	(none)
	port	<integer between 0-65535>	0
	strictmode	enabled | disabled	disabled
	optionalUserMapping	enabled | disabled	disabled
	timeout	<integer>	4
	logdetail	none | high | medium | low | trace	none
`/SP/clients/ldapssl/admingroups/`*n* where *n* is 1-5	name	<string>	(none)
`/SP/clients/ldapssl/opergroups/`*n* where *n* is 1-5	name	<string>	(none)
`/SP/clients/ldapssl/userdomains/`*n* where *n* is 1-5	domain	<string>	(none)
`/SP/clients/ldapssl/customgroups/`*n* where *n* is 1-5	name	<string>	(none)
	roles	administrator | operator | a | u| c | r | o | s	(none)
`/SP/clients/ldapssl/alternateserver/`*n* where *n* is 1-5	address	<string>	(none)
	port	<integer>	0
`/SP/clients/ldapssl/alternateservers/`*n***`/cert`** where *n* is 1-5	certstatus	<string>	(none)
	clear_action	true	(none)
	issuer	<string>	(none)
	load_uri	tftp|ftp|scp	(none)
	serial_number	<string>	(none)
	subject	<string>	(none)
	valid_from	<string>	(none)
	valid_until	<string>	(none)
	version	<string>	(none)

TABLE A-5 Targets, Properties, and Values for `set` Command *(Continued)*

Valid Targets	Properties	Values	Default
/SP/clients/ldapssl/cert/	certstatus	<string>	certificate not present
	clear_action	true	(none)
	issuer	<string>	(none)
	load_uri	tftp | ftp | scp	(none)
	serial_number	<string>	(none)
	subject	<string>	(none)
	valid_from	<string>	(none)
	valid_until	<string>	(none)
	version	<string>	(none)
/SP/clients/ldapssl/cert/*n* where *n* is 1-5	domain	<string>	(none)
/SP/clients/ntp/server/[1|2]	address	<ipaddress>	(none)
/SP/clients/radius	defaultrole	administrator | operator | a | u | c | r | o | s | none	operator
	address	<ipaddress> | none	(none)
	port	<integer>	1812
	secret	<string> | none	(none)
	state	enable | disabled	disabled
/SP/clients/smtp	address	<ipaddress>	*IP address*
	port	<integer>	25
	state	enabled | disabled	enabled
/SP/clients/syslog[1|2]	address	<ipaddress>	*IP address*
/SP/config	dump_uri	tftp | ftp | sftp | scp | http | https	(none)
	load_uri	tftp | ftp | sftp | scp | http | https	(none)
	passphrase	<string>	(none)
/SP/diag	snapshot	(none)	(none)
/SP/network	commitpending	true	(none)
	pendingipaddress	<ipaddress> | none	(none)
	pendingdiscovery	dhcp | static	dhcp
	pendingipgateway	<ipaddress> | none	(none)
	pendingipnetmask	<IP dotted decimal>	10.8.255.255
	state	enabled | disabled	enabled

TABLE A-5 Targets, Properties, and Values for `set` Command *(Continued)*

Valid Targets	Properties	Values	Default
/SP/network/ipv6	state	enabled | disabled	enabled
	autoconfig	stateless | dhcpv6_stateless | dhcpv6_stateful | disable	stateless
	pending_static_ipaddress	*<ipv6_address>*	(none)
	commitpending	true	(none)
/SP/network/test	ping	*<ipv4_address>*	(none)
	ping6	*<ipv6_address>*	(none)
/SP/preferences/banner	connect_message	<string>	(none)
	login_message	<string>	(none)
	login_message_acceptance	enabled | disabled	disabled
/SP/serial/external	commitpending	true	(none)
	flowcontrol	none	(none)
	pendingspeed	<integer from list>	9600
	speed	<integer from list>	9600
/SP/serial/host	commitpending	true	(none)
	pendingspeed	<integer from list>	9600
	speed	<integer from list>	9600
/SP/	check_physical_presence	true | false	(none)
	hostname	<string>	(none)
	reset_to_defaults	all | factory | none	(none)
	system_contact	<string>	(none)
	system_description	<string>	(none)
	system_identifier	<string>	(none)
	system_location	<string>	(none)

Examples

```
-> set /SP/users/susan role=administrator
```

```
-> set /SP/clients/ldap state=enabled binddn=proxyuser bindpw=ez24get
```

`show` Command

Use the `show` command to display information about targets and properties.

Using the `-display` option determines the type of information shown. If you specify `-display targets`, then all targets in the namespace below the current target are shown. If you specify `-display` properties, all property names and values for the target are shown. With this option you can specify certain property names, and only those values are shown. If you specify `-display all`, all targets in the namespace below the current target are shown, and the properties of the specified target are shown. If you do not specify a `-display` option, the `show` command acts as if `-display all` were specified.

The `-level` option controls the depth of the `show` command and it applies to all modes of the `-display` option. Specifying `-level 1` displays the level of the namespace where the object exists. Values greater than 1 return information for the target's current level in the namespace and the <*specified value*> levels below. If the argument is `-level all`, it applies to the current level in the namespace and everything below.

The `-o|output` option specifies the output and form of command output. ILOM only supports `-o table`, which displays targets and properties in tabular form.

The alias, `show components`, is a shortcut for the following CLI command:

```
-> show -o table -level all /SYS component state
```

The `show components` alias produces the same output as the above command. Thus, it enables you to restrict the table output to a single property below each target.

Syntax

show [*options***] [-display** *targets|properties|all***] [-level** *value|all***]** *target* **[***propertyname***]**

Options

[-d|-display] [-l|level] [-o|output]

Targets and Properties

TABLE A-6 Targets and Properties for `show` Command

Valid Targets	Properties
`/HOST/tpm`	activate enable forceclear
`/SYS`	
`/SYS/DBP/HDD`*n* where *n* is a valid HDD slot	type ipmi_name fru_name fru_manufacturer fru_version fru_serial_number controller_id disk_id capacity device_name disk_type wwn raid_status raid_ids
`/STORAGE/raid/controller@od:`*00.0* where *00.0* is the ID for the controller	fru_manufacturer fru_model pci_vendor_id pci_device_id pci_subvendor_id pci_subdevice_id raid_levels max_disks max_raids max_hot_spares max_global_hot_spares min_stripe_size max_stripe_size
`/STORAGE/raid/controller@od:`*00.0***`/`** **`raid_id`***0* where *00.0* is the ID for the controller, and **`raid_id`***0* is the target RAID disk	level status disk_capacity device_name mounted

TABLE A-6 Targets and Properties for `show` Command *(Continued)*

Valid Targets	Properties
/STORAGE/raid/controller@od:*00.0***/ raid_id***0***/disk_id***0* where *00.0* is the ID for the controller, and **raid_id***0* is the target RAID disk, and **disk_id***0* is the target disk	fru_manufacturer fru_serial_number fru_version status capacity device_name disk_type wwn raid_ids system_drive_slot
/SP	
/SP/alertmgmt/rules/ *rulename* (*rulename* = 1 through 15)	community | username destination destination_port event_class_filter event_type_filter level snmp_version type
/SP/cli	timeout
/SP/clients/ activedirectory	state certfilestatus defaultrole getcertfile address logdetail port strictcertmode timeout
/SP/clients/ activedirectory/ admingroups/*n* where *n* is 1-5	name
/SP/clients/ activedirectory/ alternateservers/*n* where *n* is 1-5	address port

TABLE A-6 Targets and Properties for show Command *(Continued)*

Valid Targets	Properties
/SP/clients/activedirectory/alternateservers/*n*/cert where *n* is 1-5	clear_action issuer load_uri serial_number subject valid_from valid_until version
/SP/clients/activedirectory/cert	certstatus clear_action issuer load_uri serial_number subject valid_from valid_until version
/SP/clients/activedirectory/customgroups/*n* where *n* is 1-5	name roles
/SP/clients/activedirectory/opergroups/*n* where *n* is 1-5	name
/SP/clients/activedirectory/userdomains/*n* where *n* is 1-5	domain
/SP/clients/dns	auto_dns nameserver searchpath
/SP/clients/ldap	binddn bindpw defaultrole address port searchbase state

TABLE A-6 Targets and Properties for `show` Command *(Continued)*

Valid Targets	Properties
`/SP/clients/ldapssl`	defaultrole address logdetail port optionalUserMapping state strictcertmode timeout
`/SP/clients/ldapssl/admingroups/`*n* where *n* is 1-5	name
`/SP/clients/ldapssl/alternateservers/`*n* where *n* is 1-5	address port
`/SP/clients/ldapssl/alternateservers/`*n***`/cert`** where *n* is 1-5	cert_status clear_action issuer load_uri serial_number subject valid_from valid_until version
`/SP/clients/ldapssl/cert`	certstatus clear_action issuer load_uri serial_number subject valid_from valid_until version
`/SP/clients/ldapssl/customgroups/`*n* where *n* is 1-5	name roles

TABLE A-6 Targets and Properties for `show` Command *(Continued)*

Valid Targets	Properties
/SP/clients/ ldapssl/ opergroups/*n* where *n* is 1-5	name
/SP/clients/ ldapssl/ userdomains/*n* where *n* is 1-5	domain
/SP/clients/ntp/server/[1|2]	address
/SP/clients/radius	address port secret state
/SP/clients/smtp	port state
/SP/clock	datetime usentpserver uptime timezone
/SP/config	dump_uri load_uri passphrase
/SP/console	escapechars
/SP/console/history	line_count pause_count start_from
/SP/diag/snapshot	dataset dump_uri result
/SP/firmware	load_uri
/SP/logs/event	clear

TABLE A-6 Targets and Properties for `show` Command *(Continued)*

Valid Targets	Properties
`/SP/network`	commitpending dhcp_server_ip ipaddress ipdiscovery ipgateway ipnetmask macaddress pendingipaddress pendingdiscovery pendingipgateway pendingipnetmask state
`/SP/network/ipv6`	state autoconfig dhcpv6_server_duid link_local_ipaddress static_ipaddress ipgateway pending_static_ipaddress dynamic_ipaddress_1
`/SP/network/test`	ping ping6
`/SP/powermgmt`	actual_power permitted_power available_power
`/SP/preferences/banner`	connect_message login_message login_message_acceptance
`/SP/serial/external`	flowcontrol speed
`/SP/serial/host`	commitpending pendingspeed speed
`/SP/services/http`	port secureredirect servicestate
`/SP/services/https`	cert_status servicestate

TABLE A-6 Targets and Properties for `show` Command *(Continued)*

Valid Targets	Properties
/SP/services/https/ssl	cert_status
/SP/services/https/ssl/default_cert	issuer subject valid_from valid_until
/SP/services/https/ssl/custom_cert	clear_action issuer load_uri subject valid_from valid_until
/SP/services/https/ssl/custom_key	key_present load_uri clear_action
/SP/services/ipmi	servicestate
/SP/services/kvms	mousemode servicestate
/SP/services/servicetag	passphrase product_urn state
/SP/services/snmp	engineid mibs port sets v1 v2c v3 servicestate
/SP/services/snmp/communities/private	permissions
/SP/services/snmp/communities/public	permissions
/SP/services/snmp/users/*username*	password role
/SP/services/ssh	state

TABLE A-6 Targets and Properties for `show` Command *(Continued)*

Valid Targets	Properties
/SP/services/ssh/keys/dsa	fingerprint length privatekey publickey
/SP/services/ssh/keys/rsa	fingerprint length privatekey publickey
/SP/services/sso	state
/SP/sessions/*sessionid*	username starttime type mode
/SP/users/*username*	role password
/SP/users/*username***/ssh/keys/1**	fingerprint algorithm load_uri clear_action embedded_comment bit_length
/SP/users/*username***/service**	service_password service_password_expires
/SP/users/*username***/escalation**	escalation_password escalation_password_expires

Examples

```
-> show /SP/users/user1
```

```
-> show /SP/clients -level2
```

```
-> show components
```

`start` Command

Use the `start` command to turn on the target or to initiate a connection to the host console. Using the `-script` option eliminates the prompt for a yes or no confirmation and the command acts as if yes were specified.

Syntax

`start [`*options*`]` *target*

Options

`[-h|help] [-script]`

Targets

TABLE A-7 Targets for `start` Command

Valid Targets	Description
`/SYS` or **`/CH`**	Starts (powers on) the system or chassis.
`/SP/console`	Starts an interactive session to the console stream.

Examples

```
-> start /SP/console
```

```
-> start /SYS
```

`stop` Command

Use the `stop` command to shut down the target or to terminate another user's connection to the host console. You will be prompted to confirm a `stop` command. Eliminate this prompt by using the `-script` option. The `-f|force` option specifies that the action will be performed immediately.

Syntax

`stop [`*options*`] [-script]` *target*

Options

`[-f|force] [-h|help]`

Targets

TABLE A-8 Targets for `stop` Command

Valid Targets	Description
/SYS or **/CH**	Perform an orderly shutdown, followed by a power off of the specified system or chassis. Use the `-f|-force` option to skip the orderly shutdown and force an immediate power off.
/SP/console	Terminate another user's connection to the host console.

Examples

```
-> stop /SP/console
-> stop -force /SYS
```

`version` Command

Use the `version` command to display ILOM version information.

Syntax

`version`

Options

`[-h|help]`

Example

```
-> version
version SP firmware version: 3.0.0
SP firmware build number: 4415
SP firmware date: Mon Mar 28 10:39:46 EST 2008
SP filesystem version: 0.1.9
```

APPENDIX **B**

Storage Redirection Command-Line Modes, Syntax, and Usage

The Storage Redirection CLI supports both an interactive and non-interactive mode for entering commands. The interactive mode is useful when you need to enter a series of Storage Redirection commands. The non-interactive mode is useful when you need to run a batch procedure or script. The syntax required for entering the Storage Redirection commands in either of these modes is as follows.

- **Interactive shell mode syntax**

  `<storageredir>` *<command> <command options> <sub-commands> <sub-command options>*

  To launch the Storage Redirection CLI and execute the commands directly from an interactive shell, you must first navigate to the location where the Storage Redirection Client was installed and launch the Storage Redirection CLI by issuing the `java -jar StorageRedir.jar` command. For instructions, see "Launch Storage Redirection CLI Using a Command Window or Terminal" on page 185.

- **Non-interactive shell mode syntax**

  `$ java -jar StorageRedir.jar` *<command> <command options> <sub-commands> <sub-command options>*

  To launch the Storage Redirection CLI and execute the commands directly from a non-interactive shell, you must enter the Storage Redirection command (`java -jar StorageRedir.jar`) at the shell prompt (`$`) followed by the commands you want to execute. For instructions, see, "Launch Storage Redirection CLI Using a Command Window or Terminal" on page 185.

Supported Storage Redirection Commands and Options

The following tables describe the supported commands and options you can issue in the Storage Redirection CLI.

- TABLE B-1 Storage Redirection Command
- TABLE B-2 Storage Redirection Command Options
- TABLE B-3 Storage Redirection Sub-Commands
- TABLE B-4 Storage Redirection Sub-Command Options

TABLE B-1 Storage Redirection Command

Command Name	Description
`java -jar StorageRedir.jar`	The `java -jar` command is used to launch the Storage Redirection client (`StorageRedir.jar`) from a command window or terminal.
`storageredir`	The `storagedir` command performs all storage redirection operations.

TABLE B-2 Storage Redirection Command Options

Option Name	Description
`- h`	The `- h` command option displays the command-line Help information.
`- v`	The `-v` command option displays the Java command version information.

TABLE B-3 Storage Redirection Sub-Commands

Sub-Command Name	Description
`list`	The `list` sub-command provides a list of the currently active storage redirections on one or all remote SPs. **Syntax usage example:** `storageredir` **`list`** `[-p storageredir_port] [remote_SP]`
`start`	The `start` sub-command invokes the specified redirection between the local host and the remote host server. If the authentication password is not provided, the system will prompt for it. **Syntax usage example:** `storageredir` **`start`** `-r redir_type -t redir_type_path -u remote_username [-s remote_user_password] [-p storageredir_port] remote_SP` **Note -** You must specify a valid Admin or Console role account in ILOM to start the redirection of storage device on a remote server.
`stop`	The `stop` sub-command stops the specified redirection between the local host and the remote host server. If the authentication password is not provided, the system will prompt for it. **Syntax usage example:** `storageredir` **`stop`** `-r redir_type -u remote_username [-s remote_user_password] [-p storageredir_port] remote_SP` **Note -** You must specify a valid Admin or Console role account in ILOM to stop the redirection of storage device on a remote server.
`test-service`	The `test-service` sub-command verifies whether the storage redirection service connection is active on the local host. **Syntax usage example:** `storageredir` **`test-service`** `[-p storageredir_port]`
`stop-service`	The `stop-service` sub-command stops the storage redirection service connection to the remote host server. **Syntax usage example:** `storageredir` **`stop-service`** `[-p storageredir_port]`

TABLE B-4 Storage Redirection Sub-Command Options

Sub-Command Option Name	Description
`-r` *redir_type*	The `-r` *redir_type* identifies the type of storage media being redirected. Valid device values for *redir_type* include: • CD-ROM device Syntax: `-r cdrom` • CD-ROM image: Syntax: `-r cdrom_img` • Floppy device: Syntax: `-r floppy` • Floppy image: Syntax: `-r floppy_img`
`-t` *redir_type_path*	The `-t` *redir_type_path* identifies the full path to where the storage redirection media is stored or mounted. Example: `-t /home/username/JRC_Test_Images/CDROM.iso`
`-u` *remote_username*	The `-u` *remote_username* identifies the user name required to log in to the ILOM SP. Example: `-u` *john_smith* **Note -** Any valid user account in ILOM can install or launch the Storage Redirection service or client on their local system. However, a valid Admin or Console role in ILOM is required to start or stop the redirection of a storage device on a remote server.
`-s` *remote_user_password*	The `-s` *remote_user_password* identifies the password required to log in to the ILOM SP. If this password command is not specified at the command line, the system will automatically prompt you for it.
`-p` *storageredir_port*	The `-p` *storageredir_port* identifies the storage redirection communication port on the local host. The default port provided is 2121. Example: `-p 2121`

APPENDIX **C**

Diagnosing IPv4 or IPv6 ILOM Connection Issues

If you are experiencing difficulties with connecting to ILOM when using IPv6, see TABLE C-1 to help resolve common problems when accessing ILOM using IPv6.

TABLE C-1 Common IPv6 Connection Problems and Suggested Resolutions

IPv6 Common Connection Problem	Suggested Resolution
Unable to access the ILOM web interface using an IPv6 address.	Ensure that the IPv6 address in the URL is enclosed by brackets, for example: `https://[fe80::221:28ff:fe77:1402]`
Unable to download a file using an IPv6 address.	Ensure that the IPv6 address in the URL is enabled by brackets, for example: `load -source tftp://[fec0:a:8:b7:214:rfff:fe01:851d]desktop.pkg`
Unable to access ILOM using IPv6 from a network client.	If on a separate subnet, try the following: • Verify that ILOM has a dynamic or static address (not just a Link-Local address). • Verify that the network client has IPv6 address configured (not just a Link-Local address). If on the same or separate subnet, try the following • Ensure that setting for `IPv6 State` is enabled on the Network Settings Page in the ILOM web interface or under the `/SP/network/ipv6` target in the ILOM CLI. • Run `ping6` in a restricted shell. • Run `traceroute` in a restricted shell.

TABLE C-1 Common IPv6 Connection Problems and Suggested Resolutions *(Continued)*

IPv6 Common Connection Problem	**Suggested Resolution**
Unable to access ILOM from a client within a dual-stack IPv4 and IPv6 network environment.	Ensure that the following settings are enabled: • `State` – You can enable the setting for `State` on the Network Settings page in the ILOM web interface or under the `/SP/network` target in the CLI. • **`IPv6 State`** – You can enable the setting for `IPv6 State` on the Network Settings page in the ILOM web interface or under the `/SP/network/ipv6` target.
Unable to access ILOM using IPv4 from a network client.	Ensure that the setting for `State` is enabled on the Network Settings page in the ILOM web interface or under the `/SP/network` target in the ILOM CLI.

APPENDIX **D**

Manual Host OS Configuration Guidelines for Local Interconnect Interface

If you chose to manually configure a non-routable IPv4 address for the ILOM SP connection point on the Local Interconnect Interface, you will also need to manually configure a non-routable IPv4 address for the host OS connection point on the Local Interconnect Interface. General guidelines, per operating system, for configuring a static non-routable IPv4 address for the host OS connection point are provided in this appendix. For additional information about configuring IP addresses on the host operating system, consult the vendor operating system documentation.

Note – ILOM will present the internal USB Ethernet device installed on your server as an USB Ethernet interface to the host operating system.

TABLE D-1 General Guidelines for Configuring Internal USB Ethernet Device on Host OS

Operating System	General Guidelines
Windows Server 2008	After Windows discovers the internal USB Ethernet device, you will most likely be prompted to identify a device driver for this device. Since no driver is actually required, identifying the `.inf` file should satisfy the communication stack for the internal USB Ethernet device. The `.inf` file is available from the Oracle Hardware Management Pack 2.1.0 software distribution. You can download this management pack software from the Oracle software product download page (`www.oracle.com`) as well as extract the `.inf` file from the Management Pack software. For additional information about extracting the `.inf` file from the Management Pack software, see the *Oracle Server Hardware Management Pack User's Guide* (821-1609). After applying the `.inf` file from the Oracle Hardware Management Pack 2.1.0 software distribution, you can then proceed to configure a static IP address for the host OS connection point of the Local Interconnect Interface by using the Microsoft Windows Network configuration option located in the Control Panel (Start --> Control Panel). For more information about configuring an IPv4 address in Windows 2008, see the Microsoft Windows Operating System documentation or the Microsoft Tech Net site (`http://technet.microsoft.com/en-us/library/cc754203%28WS.10%29.aspx`).

Linux	Most supported Linux operating system installations on an Oracle Sun server include the installation of the device driver for an internal Ethernet device.
	Typically, the internal USB Ethernet device is automatically discovered by the Linux operating system. The internal Ethernet device typically appears as `usb0`. However, the name for the internal Ethernet device might be different based on the distribution of the Linux operating system.
	The instructions below demonstrate how to configure a static IP address corresponding to `usb0`, which typically represents an internal USB Ethernet device found on the server:
	`\>lsusb usb0`
	`\> ifconfig usb0 169.254.182.77`
	`\> ifconfig usb0 netmask 255.255.255.0`
	`\> ifconfig usb0 broadcast 169.254.182.255`
	`\> ifconfig usb0`
	`\> ip addr show usb0`
	Note - Rather than performing the typical `ifconfig` steps, it is possible to script the configuration of the interface. However, the exact network scripts vary among the Linux distributions. Typically, the operating version of Linux will have examples to model the network scripts.
	For more information about how to configure an IP address for device using a Linux operation system, see the Linux operating system documentation.

TABLE D-1 General Guidelines for Configuring Internal USB Ethernet Device on Host OS *(Continued)*

Operating System	General Guidelines

Solaris	Most Solaris Operating System installations on a Oracle Sun platform server include the installation of the device driver for an internal USB Ethernet device. If this driver was not supported, you can extract this driver from the Oracle Hardware Management Pack 2.1.0 or later software. For information about how to extract the Solaris-specific OS driver for the Ethernet interface, see the *Oracle Server Hardware Management Pack User's Guide* (821-1609).
	Typically, the internal USB Ethernet device is automatically discovered by the Solaris Operating System. The internal Ethernet device typically appears as `usbecm0`. However, the name for the internal Ethernet device might be different based on the distribution of the Solaris Operating System.
	After the Solaris Operating System recognizes the local USB Ethernet device, the IP interface for the USB Ethernet device needs to be configured.
	The following instructions demonstrate how to configure a static IP address corresponding to `usbecm0`, which typically represents an internal USB Ethernet device found on the server.
	• Type the following command to `plumb` the IP interface or `unplumb` the IP interface:
	`ifconfig usbecm0 plumb`
	`ifconfig usbecm0 unplumb`
	• Type the following commands to set the address information:
	`ifconfig usbecm0 netmask 255.255.255.0 broadcast 169.254.182.255 169.254.182.77`
	• To set up the interface, type:
	`ifconfig usbecm0  up`
	• To bring the interface down, type:
	`ifconfig usbecm0  down`
	• To show the active interfaces, type:
	`ifconfig -a`
	• To test connectivity, ping the Solaris host or the SP internal USB Ethernet device.
	`ping` *<IPv4 address of Solaris Host>*
	`ping` *<IPv4 address of SP-Ethernet USB>*
	Note - Rather than performing the typical `ifconfig` steps, it is possible to script the configuration of the interface. However, the exact network scripts can vary among the Solaris distributions. Typically, the operating version will have examples to model the network scripts.
	For more information about how to configure a static IP address for a device using the Solaris Operating System, see the Solaris Operating System documentation.

Note – If the internal USB Ethernet device driver was not included in your operating system installation, you can obtain the device driver for the Ethernet device from the Oracle Hardware Management Pack 2.1.0 or later software. For more information about extracting this file from the Management Pack, see the *Oracle Server Hardware Management Pack User's Guide* (821-1609).

Index