Oracle Integrated Lights Out Manager (ILOM) 3.0

Daily Management – Web Procedures Guide

Part No.: E21446-02
August 2012

Please
Recycle

Adobe PostScript™

Contents

Using This Documentation

This web interface procedures guide describes the Oracle Integrated Lights Out Manager (ILOM) daily management features that are common to Oracle's Sun rackmounted servers, server modules, and CMMs supporting Oracle ILOM 3.0.

For further information about the features presented in this guide, use this guide in conjunction with other guides in the Oracle ILOM 3.0 Documentation Library. This guide is written for technicians, system administrators, authorized service providers, and users who have experience managing system hardware.

This chapter includes the following topics:

Related Documentation

Documentation	Links
All Oracle products	`http://www.oracle.com/documentation`
Oracle Integrated Lights Out Manager (ILOM) 3.0 Documentation Library	`http://www.oracle.com/pls/topic/lookup?ctx=ilom30`

Documentation	Links
System management, single system management (SSM) security, and diagnostic documentation	http://www.oracle.com/technetwork/documentation/sys-mgmt-networking-190072.html
Oracle Hardware Management Pack 2.0	http://docs.oracle.com/cd/E19960-01/index.html

Note: To locate Oracle ILOM 3.1 documentation that is specific to your Sun server platform, see the Oracle ILOM section of the administration guide that is available for your server.

Documentation Feedback

Provide feedback on this documentation at:

http://www.oracle.com/goto/docfeedback

Oracle ILOM 3.0 Version Numbers

Oracle ILOM 3.0 uses a firmware version numbering scheme that helps you to identify the firmware version you are running on your server or CMM. This numbering scheme includes a five-field string, for example, `a.b.c.d.e`, where:

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

For example, Oracle ILOM 3.1.2.1.a would designate:

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

Tip – To identify the Oracle ILOM firmware version installed on your Sun server or CMM, click System Information --> Versions in the web interface, or type `version` in the command-line interface.

Support and Accessibility

Description	Links

Access electronic support through My Oracle Support	`http://support.oracle.com`
	For hearing impaired:
	`http://www.oracle.com/accessibility/support.html`

Learn about Oracle's commitment to accessibility	`http://www.oracle.com/us/corporate/accessibility/index.html`

Web Interface Overview

Description	Links
Identify requirements for using Oracle ILOM’s web interface	• “About the Web Interface” on page 1 • “Browser and Software Requirements” on page 2
Compare Oracle ILOM’s server SP and CMM web interface components	• “CMM and Server SP Web Interface Connection” on page 4
Learn about Oracle ILOM’s web interface tabs and the functions you perform from them	• “Web Interface Navigation Tabs” on page 8

Related Information

- *Oracle ILOM 3.0 Daily Management Concepts*, Oracle ILOM overview
- *Oracle ILOM 3.0 Daily ManagementCLI Procedures*, CLI overview
- *Oracle ILOM 3.0 Protocol Management Reference* , SNMP overview
- *Oracle ILOM 3.0 Protocol Management Reference*, IPMI overview
- *Oracle ILOM 3.0 Maintenance and Diagnostics*, maintenance and diagnostics overview
- *Oracle ILOM 3.0 Feature Updates and Release Notes*, new or updated features

About the Web Interface

The Oracle ILOM web interface is accessible through a browser and uses a standard interface. The Oracle ILOM web interface enables you to monitor and manage local and remote systems. One of the most powerful features of Oracle ILOM is the ability to redirect the server's graphical console to a local workstation or laptop system. When you redirect the host console, you can configure the local system's keyboard and mouse to act as the server's keyboard and mouse. You can also configure the diskette drive or CD-ROM drive on the remote system as a device virtually connected to your Oracle Sun system. You can access these features using the Oracle ILOM Remote Console application.

Browser and Software Requirements

Refer to the following topics for a list of supported web browsers and network addresses accepted by the Oracle ILOM web interface.

- "Supported Web Browsers" on page 2
- "Network Addresses Accepted by Oracle ILOM" on page 3

Supported Web Browsers

The web interface has been tested successfully with recently released Mozilla Firefox, and Internet Explorer web browsers, and may be compatible with other web browsers.

Oracle ILOM supports the browsers listed in the following table.

TABLE: Supported Web Browsers

Operating System	Web Browser
Oracle Solaris (9 and 10)	• Mozilla 1.4 and 1.7 • Firefox 1.x and later
Linux (Red Hat, SuSE, Ubuntu, Oracle)	• Mozilla 1.x and later • Firefox 1.x and later • Opera 6.x and later
Microsoft Windows (98, 2000, XP, Vista)	• Internet Explorer 5.5, 6.x, and 7.x • Mozilla 1.x and later • Firefox 1.x and later • Opera 6.x and later
Macintosh (OSX v10.1 and above)	• Internet Explorer 5.2 • Mozilla 1.x and later • Firefox 1.x and later • Safari – all

Note – Oracle ILOM comes preinstalled on your Sun system and includes the Remote Console application. To run the Oracle ILOM Remote Console, you must have the Java 1.5 Runtime Environment (JRE 1.5) or later version of the JRE software installed on your local client. To download the JRE software, go to `http://java.com`. For a list of web browsers and operating systems supported by the Oracle ILOM Remote Console, refer to the *Oracle ILOM 3.0 Remote Redirection Consoles CLI and Web Guide*.

Network Addresses Accepted by Oracle ILOM

As of Oracle ILOM 3.0.12 or later, the following network addresses are accepted by the Oracle ILOM interfaces.

Note – When entering an IPv6 address or Link-Local IPv6 address, the address must be enclosed within brackets to work correctly.

- **IPv4 address**. `10.8.183.106`
- **IPv6 address**. `[fec0:a:8:b7:214:4fff:5eca:5f7e/64]`
- **Link-Local IPv6 address**. `[e80::214:4fff:feca:5f7e/64]`
- **DNS host domain address**. `company.com`

Examples for Entering an IPv6 Address

When you specify an IPv6 address in a URL with a web browser or when you transfer a file, the IPv6 address *must be enclosed* in brackets to work correctly. When you specify an IPv6 address to log in to Oracle ILOM using an SSH connection, the IPv6 address should *not be enclosed* in brackets.

Examples:

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

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

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

  `ssh root@`*ipv6address*

  Note that when you specify an IPv6 address to log in to Oracle ILOM using an SSH connection, the IPv6 address should *not be enclosed* in brackets.

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

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

For additional information about entering IPv6 addresses, refer to the *Oracle ILOM 3.0 Daily Management – Concepts Guide*. For help with diagnosing IPv4 and IPv6 connection issues, see "Diagnosing IPv4 or IPv6 Oracle ILOM Connection Issues" on page 145.

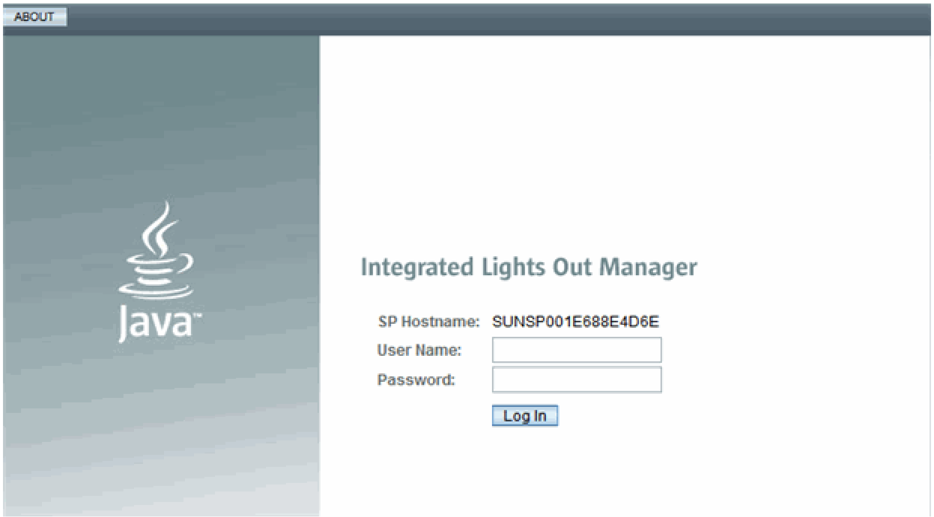
CMM and Server SP Web Interface Connection

Topics discussed in this section include:

- "Oracle ILOM Welcome Page" on page 4
- "Server SP Web Interface Components" on page 5
- "CMM Web Interface" on page 6

Oracle ILOM Welcome Page

To establish a web interface connection to Oracle ILOM on the CMM or server SP, specify the IP address of the CMM or server SP in the web browser. A welcome page appears prompting you to enter a user name and password.



Integrated Lights Out Manager

SP Hostname: SUNSP001E688E4D6E

User Name:

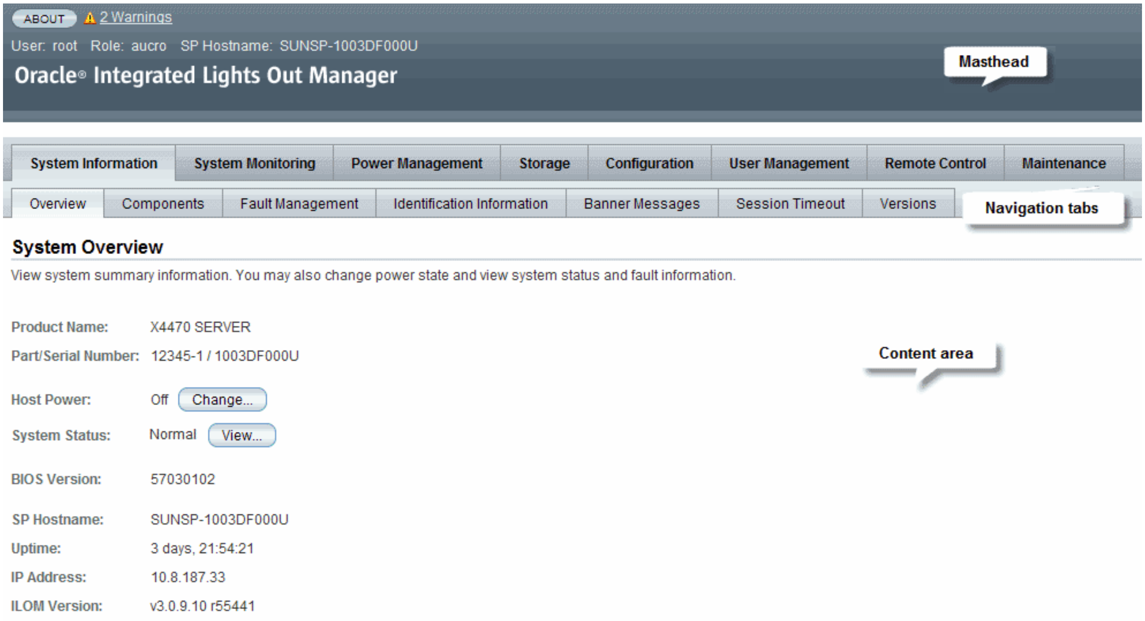
Password:

Server SP Web Interface Components

The main Oracle ILOM web page for the server SP organizes the settings you can view or configure for that server within the tabs appearing at the top of the page, as shown in the following example. For a description of the CMM Oracle ILOM web interface, see “CMM Web Interface” on page 6.

Note – The Oracle ILOM web interface navigation tabs differ slightly depending on the Oracle ILOM features implemented on a specific platform and on the Oracle ILOM version currently installed on your system. Therefore, you might have access to different tabs from those described in this section. For information about the Oracle ILOM interface for your system, refer to your Oracle ILOM supplement or platform administration guide.

FIGURE: Oracle ILOM Web Interface Main Page



User: root Role: aucro SP Hostname: SUNSP-1003DF000U

Oracle® Integrated Lights Out Manager

System Overview

View system summary information. You may also change power state and view system status and fault information.

Product Name: X4470 SERVER
Part/Serial Number: 12345-1 / 1003DF000U
Host Power: Off
System Status: Normal
BIOS Version: 57030102
SP Hostname: SUNSP-1003DF000U
Uptime: 3 days, 21:54:21
IP Address: 10.8.187.33
ILOM Version: v3.0.9.10 r55441

Each web interface page has three main sections: the masthead, the navigation tabs, and the content area.

The masthead provides the following buttons and information on each page of the web interface:

- **About button** – Click to view product and copyright information.

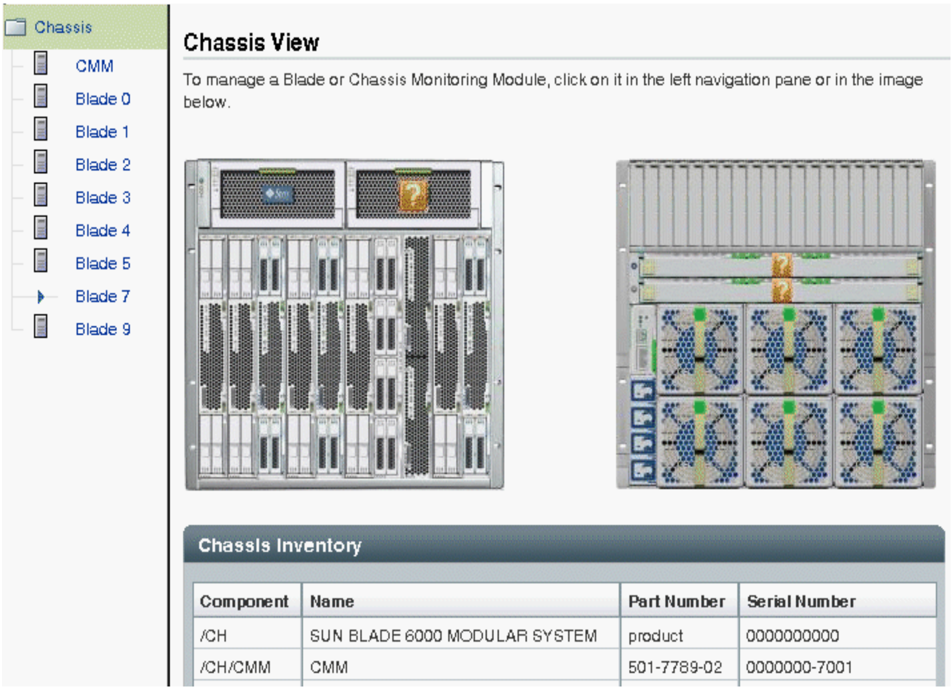
- **User field** – Displays the user name of the current user of the web interface and the user’s role.
- **Server field** – Displays the host name of the Oracle ILOM SP or CMM.
- **Refresh button** – Click to refresh the information in the content area of the page. The Refresh button does not save new data that you might have entered or selected on the page.
- **Log Out button** – Click to end the current session of the web interface.

The Oracle ILOM web interface navigation structure includes first and second-level tabs that you can click to open a specific page. For example, when you click a first-level tab, one or more second-level tabs might display that provide you with further options. The content area is where you find information about a specific feature or operation.

CMM Web Interface

The Oracle ILOM web page for the CMM includes:

- The **Navigation pane** on the left side of the screen that lists visible entries only for components that are present and manageable in the chassis.
- A **Chassis view and inventory table** appear on the right side of the screen when the Chassis entry in the navigation pane is selected. The Chassis view displays the front and rear view of the chassis. The Chassis Inventory table provides information about the manageable chassis components present in the chassis.



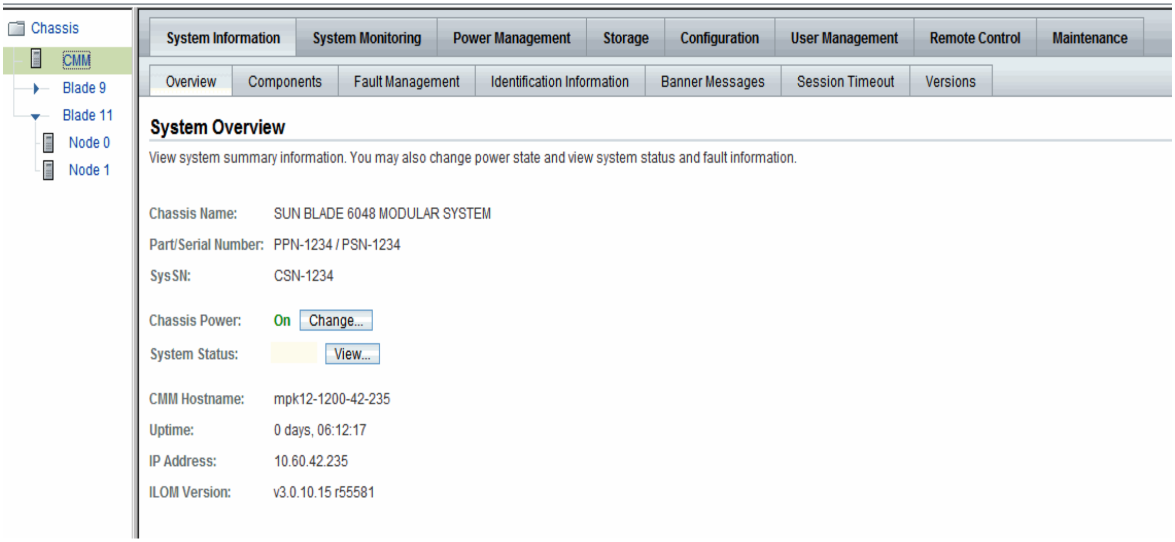
Chassis View

To manage a Blade or Chassis Monitoring Module, click on it in the left navigation pane or in the image below.

Chassis Inventory

Component	Name	Part Number	Serial Number
/CH	SUN BLADE 6000 MODULAR SYSTEM	product	0000000000
/CH/CMM	CMM	501-7789-02	0000000-7001

- The **CMM management settings** appear in the right side of the screen when a CMM entry is selected in the navigation pane. The settings you can view or configure for the CMM are organized in the eight tabs appearing at the top of the page, as shown in the following example.



System Overview

View system summary information. You may also change power state and view system status and fault information.

Chassis Name: SUN BLADE 6048 MODULAR SYSTEM

Part/Serial Number: PPN-1234 / PSN-1234

SysSN: CSN-1234

Chassis Power: On

System Status:

CMM Hostname: mpk12-1200-42-235

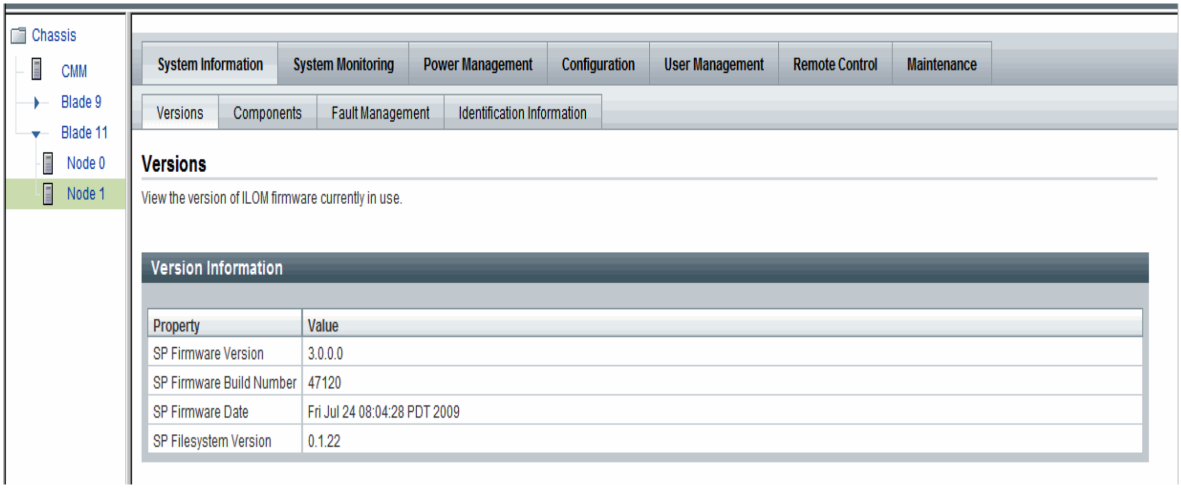
Uptime: 0 days, 06:12:17

IP Address: 10.60.42.235

ILOM Version: v3.0.10.15 r55581

Note – For details about the CMM Zoning Management features available in Oracle ILOM as 3.0.10, refer to the *Oracle ILOM) 3.0 CMM Administration Guide For Sun Blade 6000 and Sun Blade 6048 Modular Systems*.

- The **Blade management settings** appear in the right side of the screen when a blade entry in the navigation pane is selected. If you are managing a blade with multiple Service Processors (SPs), an **Node** entry for each dedicated SP appears in the navigation pane, as shown in the following example.



Versions

View the version of ILOM firmware currently in use.

Version Information

Property	Value
SP Firmware Version	3.0.0.0
SP Firmware Build Number	47120
SP Firmware Date	Fri Jul 24 08:04:28 PDT 2009
SP Filesystem Version	0.1.22

The settings you can view or configure for an individual blade SP are organized in the seven tabs appearing in the right side of the Oracle ILOM Web Interface page, as shown in the previous example.

For more information about the tabs described in this section, see "Web Interface Navigation Tabs" on page 8.

Web Interface Navigation Tabs

Topics discussed in this section include:

- "Navigation Tab Descriptions" on page 9
- "Jump Links" on page 13

Navigation Tab Descriptions

The following table describes the web interface tabs that you can use to access Oracle ILOM functions.

Note – The Oracle ILOM web interface navigation tabs differ slightly depending on the Oracle ILOM features implemented on a specific server platform and on the Oracle ILOM firmware version currently installed on your server or CMM. Therefore, you might have access to different tabs from those described in the following table. For information about the Oracle ILOM interface for your system, refer to your Oracle ILOM supplement or platform administration guide.

First-level Tab	Second and Third-level Tabs	What You Can Do	Applicable To
System Information			
	Overview	View the product name, part or serial number, host power state, system status state, BIOS version, SP host name, system uptime, IP address, and Oracle ILOM version that is running. • Host Power state offers you the ability to control the system power state • System Status state offers you the ability to view faulted hardware • SysFW Information (SPARC only) indicates the system firmware version embedded on the server	Server SP CMM
	Components	View the names, types, and status of the components that Oracle ILOM is monitoring.	Server SP CMM
	Fault Management	View information about components that are in a faulted state.	Server SP CMM
	Identification Information	Enter or change the service processor identification information by assigning a host name or system identifier.	Server SP CMM
	Banner Messages	View and configure a message that appears prior to log in and login message that appears after user log-in.	Server SP CMM
	Session Timeout	View the session time-out or change the session time-out parameter.	Server SP CMM

First-level Tab	Second and Third-level Tabs	What You Can Do	Applicable To
	Versions	View the SP file system version, the SP firmware version, SP firmware build number, and SP firmware date.	Server SP CMM
System Monitoring			
	Sensor Readings	View the name, type, and reading of the sensors.	Server SP CMM
	Indicators	View the name and status of the indicators and LEDs.	Server SP CMM
	Event Logs	View various details about each particular event, including the event ID, class, type, severity, date and time, and description of the event.	Server SP CMM
Power Management			
	Consumption	View power consumption metrics for actual power and permitted power, as well as set power consumption thresholds to generate email alerts or SNMP notifications.	Server SP CMM
	Allocation	View system power requirements for capacity planning. This tab was previously named Distribution prior to Oracle ILOM 3.0.10.	Server SP CMM
	Limit	View or configure server power limits. This tab was previously named Budget prior to Oracle ILOM 3.0.8.	Server SP
	Settings	Configure policy options for power consumption on SPARC servers.	SPARC
	Redundancy	View and configure CMM power supply redundancy options. This tab became available as of Oracle ILOM 3.0.6.	CMM
	Statistics	View power statistical data for CMM and server modules (blades).	CMM
	History	View a history of rolling averages for power consumption.	Server SP CMM
Storage			

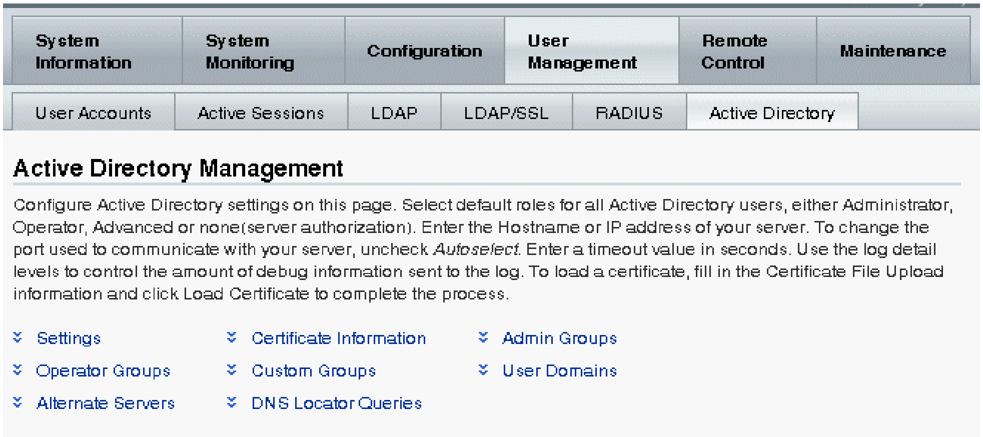
First-level Tab	Second and Third-level Tabs	What You Can Do	Applicable To
	RAID --> Controllers	View information for RAID controllers. To get further details, click the controller name.	Server SP
	RAID --> Disks	View information for all disks attached to RAID controllers. To view further details, click the disk name.	Server SP
	RAID --> Volumes	View information for RAID volumes. To view further details, click the volume name.	Server SP
	Zoning	Enable or disable Zone Manager settings and reset the Zone Manager password.	CMM
Configuration			
	System Management Access --> Web Server	Edit or update the web server settings, such as the HTTP web server or the HTTP port.	Server SP CMM
	System Management Access --> SSL Certificate	View information about the default SSL certificate, or optionally find and enter a new SSL certificate.	Server SP CMM
	System Management Access --> SNMP	Edit or update SNMP settings	Server SP CMM
	System Management Access --> SSH Server	Configure Secure Shell (SSH) server access and key generation.	Server SP CMM
	System Management Access --> IPMI	Use a command-line interface to monitor and control your server platform, as well as to retrieve information about your server platform.	Server SP CMM
	System Management Access --> CLI	Configure the CLI settings. The Session Time-out value indicates the number of idle minutes that can lapse before automatic CLI logout occurs.	Server SP CMM
	System Management Access --> WS-Man	Configure the WS-Management settings. WS-Management is a Web Services and SOAP-based protocol for managing servers and devices.	Server SP
	Alert Management	View details about each alert and change the list of configured alerts.	Server SP CMM
	Network	View and edit the IPv4 and IPv6 network settings for Oracle ILOM and for local interconnect interface settings.	Server SP CMM
	DNS	Specify host names, and have those host names resolved into IP addresses using the Domain Name Service (DNS).	Server SP CMM

First-level Tab	Second and Third-level Tabs	What You Can Do	Applicable To
	Serial Port	View and edit the baud rate of the internal and external serial ports.	Server SP CMM
	Clock	View and edit the Oracle ILOM clock time manually, or synchronize the Oracle ILOM clock with an NTP server.	Server SP CMM
	Timezone	Specify a particular timezone so that timestamps displayed by the service processor can be correlated to logs created elsewhere (for example, in the Oracle Solaris Operating System).	Server SP CMM
	Syslog	Configure the server addresses to which the syslog messages will be sent.	Server SP CMM
	SMTP Client	Configure the state of the SMTP client, which is used for sending email notifications of alerts.	Server SP CMM
	Policy	Enable or disable settings that control the behavior of the system, such as power-on policies.	Server SP CMM
User Management			
	Active Sessions	View the users currently logged in to Oracle ILOM, as well as the type of session users have initiated.	Server SP CMM
	User Accounts	Add, delete, or modify local Oracle ILOM user accounts.	Server SP CMM
	LDAP	Configure Oracle ILOM access for LDAP users.	Server SP CMM
	LDAP/SSL	Configure Oracle ILOM access for LDAP users with enhanced security settings enabled by Secure Socket Layer (SSL) technology.	Server SP CMM
	RADIUS	Configure Oracle ILOM access for RADIUS users.	Server SP CMM
	Active Directory	Configure Oracle ILOM access for Active Directory users	Server SP CMM
Remote Control			
	Redirection	Manage the host remotely by redirecting the system console to your local machine.	Server SP CMM

First-level Tab	Second and Third-level Tabs	What You Can Do	Applicable To
	KVMS	Enable or disable the remote management state of the keyboard, video, mouse, or storage device.	Server SP
	Remote Power Control	Select a power state: Immediate Power Off, Graceful Shutdown and Power Off, Power On, Power Cycle, or Reset.	Server SP CMM
	Diagnostics	Enable or disable diagnostics for x64 processor-based systems or SPARC processor-based systems.	Server SP
	Host Control	View and configure the host control information. Configure the boot device at the next system power-on.	Server SP
Maintenance			
	Firmware Upgrade	Start the process to obtain an upgrade of the Oracle ILOM firmware.	Server SP CMM
	Backup/Restore	Backup and restore the service processor configuration to a remote host or removable storage device in a secure manner.	Server SP CMM
	Reset SP	Reset the service processor.	Server SP
	Configuration Management	Manage the service processor configuration data.	Server SP CMM
	Reset Components	Reset chassis monitoring modules and service processors.	CMM
	Snapshot	Collect environmental, log, error, and FRUID data and send it to a USB thumb drive, an external host using CLI, or as a downloaded file.	Server SP CMM

Jump Links

As of Oracle ILOM 3.0.3, jump links were added on some web pages for easier navigation to sub-sections within a page. An example of an Oracle ILOM web page that includes jump links is shown in the following figure.



Active Directory Management

Configure Active Directory settings on this page. Select default roles for all Active Directory users, either Administrator, Operator, Advanced or none(server authorization). Enter the Hostname or IP address of your server. To change the port used to communicate with your server, uncheck *Autoselect*. Enter a timeout value in seconds. Use the log detail levels to control the amount of debug information sent to the log. To load a certificate, fill in the Certificate File Upload information and click Load Certificate to complete the process.

Logging In to and Out of Oracle ILOM and Displaying Banner Messages (Web)

Description	Links
Identify requirements for logging into to Oracle ILOM.	• "Before Your Initial Login" on page 16
Procedure for logging in to Oracle ILOM using the default root user account	• "Log In Using the Root User Account (Web)" on page 17
Procedure for logging in to Oracle ILOM using a user account	• "Log In to Oracle ILOM With User Account (Web)" on page 18
Procedure for logging out of Oracle ILOM	• "Log Out of Oracle ILOM (Web)" on page 19
Procedure for configuring banner messages to appear on the Oracle ILOM Login page	• "Display Banner Messages on Login Page (Web)" on page 19

Related Information

- *Oracle ILOM 3.0 Quick Start*, logging in to Oracle ILOM
- *Oracle ILOM 3.0 Quick Start*, mandatory setup tasks (web)
- *Oracle ILOM 3.0 Daily Management CLI Procedures*, logging in to Oracle ILOM
- *Oracle ILOM 3.0 Daily Management CLI Procedures*, banner messages
- *Oracle ILOM 3.0 Daily Management Concepts*, banner messages

Before Your Initial Login

Prior to performing the procedures in this section, you should ensure that the following requirements are met.

- Ensure that a physical network management connection to the system (server or CMM) is established. For instructions about how to establish a physical connection to the SER MGT or NET MGT port on your system, refer to the installation guide provided with your server or CMM.

  The login procedures in this section assume you are logging in to the Oracle ILOM web interface through a physical network connection.

Note – Alternatively, for Oracle Sun servers supporting a Local Interconnect Interface connection, you can connect directly to ILOM from the host operating system. For more details about connecting to ILOM using a Local Interconnect Interface connection, see "Configuring the Local Interconnect Interface (Web)" on page 38.

- Obtain the server SP or CMM network address.

  Oracle ILOM, by default, will automatically attempt to obtain and assign an IPv4 or IPv6 address for the server SP or CMM. To determine the default IP address assigned to the server SP or CMM, establish a local serial management connection to the server SP or CMM and view the /network (or /network/ipv6) properties.

  For more information about how to establish a local serial management connection to Oracle ILOM, refer to the Oracle ILOM 3.0 Quick Start Guide or refer to the documentation provided with your Sun server or Sun blade chassis system

  For information about modifying the default IP address assigned to your server SP or CMM, see "Configuring Network Settings (Web)" on page 22.

- Obtain an Oracle ILOM user account.

  If you are setting up Oracle ILOM for this first-time, use the default **root** account and **changeme** password to log in. It is highly recommended after your system is set up that a new user account is created for each Oracle ILOM user. For more information about setting up user accounts, see "Configuring User Accounts (Web)" on page 44.

▼ Log In Using the Root User Account (Web)

1. **In the web browser address bar, type the network address for the server SP or CMM.**

   Examples:

   - IPv4 network address example:

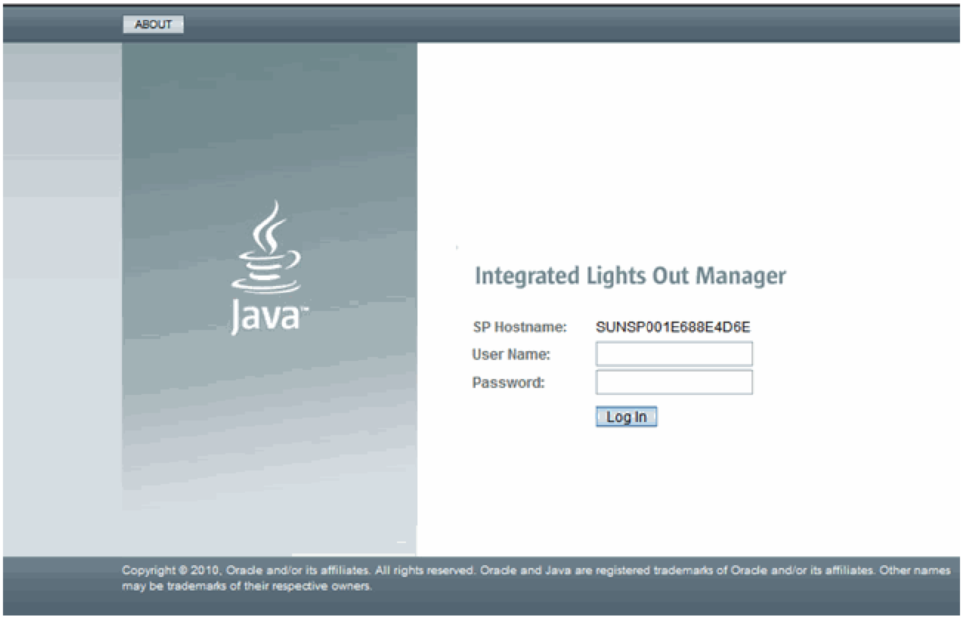
     `http://10.8.183.106`

   - IPv6 network address example:

     `http://[fec0:a:8:b7:214:4fff:5eca:5f7e/64]`

   For more information about network addresses accepted by Oracle ILOM, see "Network Addresses Accepted by Oracle ILOM" on page 3. For help with diagnosing Oracle ILOM connection issues, see "Diagnosing IPv4 or IPv6 Oracle ILOM Connection Issues" on page 145.

   The web interface Login page appears.



Integrated Lights Out Manager

SP Hostname: SUNSP001E688E4D6E

User Name:

Password:

Copyright © 2010, Oracle and/or its affiliates. All rights reserved. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

2. **Type the `root` user name and password. For instance, the default `root` user name and password provided with Oracle ILOM are as follows:**

   User name: **`root`**

   Password: **`changeme`**

3. **Click Log In.**

   The Version page in the web interface appears.

▼ Log In to Oracle ILOM With User Account (Web)

1. **In the web browser address bar, type the network address for the server SP or CMM.**

   Examples:

   - IPv4 network address example:

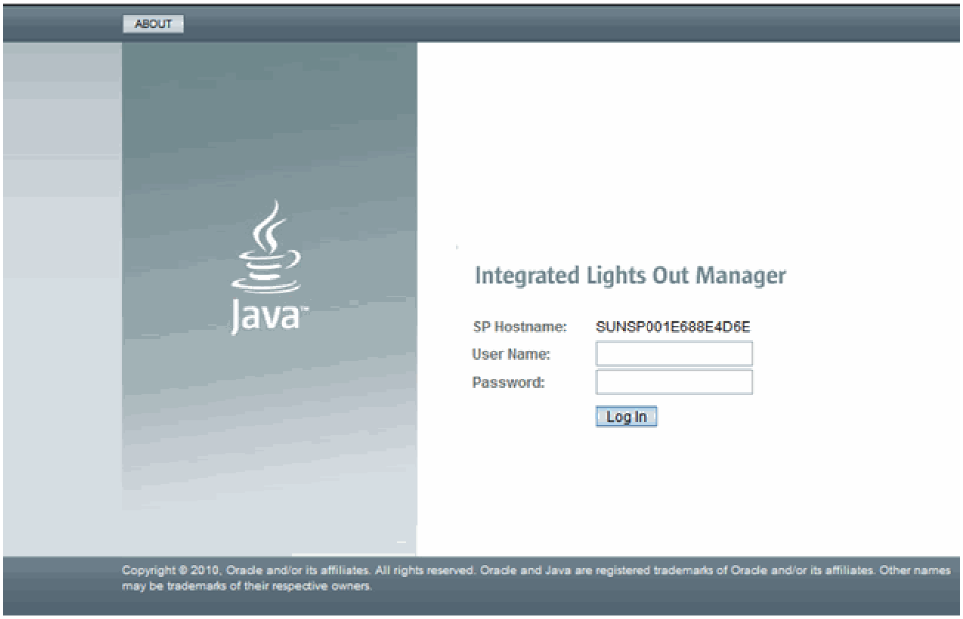
     `http://10.8.183.106`

   - IPv6 network address example:

     `http://[fec0:a:8:b7:214:4fff:5eca:5f7e/64]`

   For more information about network addresses accepted by Oracle ILOM, see "Network Addresses Accepted by Oracle ILOM" on page 3. For help with diagnosing Oracle ILOM connection issues, see "Diagnosing IPv4 or IPv6 Oracle ILOM Connection Issues" on page 145.

   The web interface Login page appears.


ABOUT
Java
Integrated Lights Out Manager
SP Hostname:
SUNSP001E688E4D6E
User Name:
Password:
Log In
Copyright © 2010, Oracle and/or its affiliates. All rights reserved. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

2. **Type your Oracle ILOM user name and password.**

3. **Click Log In.**

   The Oracle ILOM web interface appears, displaying the Version page.

▼ Log Out of Oracle ILOM (Web)

- **Click the Log Out button in the Oracle ILOM web interface.**

  The Log Out button is located in the top right corner of the web interface. Do not use the Log Out button on your web browser to exit Oracle ILOM.

▼ Display Banner Messages on Login Page (Web)

Before You Begin

- The Admin (a) role is required for you to configure banner messages in Oracle ILOM.
- The server must be running Oracle ILOM firmware version 3.0.8 or later.

Follow these steps to configure banner messages.

1. **Log in to the Oracle ILOM SP web interface or the Oracle ILOM CMM web interface.**
2. **In the Oracle ILOM web interface, click System Information --> Banner Messages.**
3. **In the Banner Message page, do the follow:**

Task	Instructions
To create a banner message to appear on the Login page	Enter the message in the Connect Message text box.
To create banner message to appear in a dialog box after users log in to Oracle ILOM.	Enter the message in the Login Message text box.

4. **Click Message Acceptance check box to enable the system to display the banner message(s).**
5. **Click Save.**

Configuring Network, Secure Shell, and Local Interconnect Settings (Web)

Description	Links
Configure network properties for IP, host name, DNS, serial port output, as well as HTTP web access.	• "Configuring Network Settings (Web)" on page 22
Manage secure shell settings.	• "Configuring Secure Shell Settings" on page 37
Manage the local interconnect interface settings in Oracle ILOM	• "Configure the Local Interconnect Interface (Web)" on page 40

Related Information

- *Oracle ILOM 3.0 Quick Start*, establish a network management connection
- *Oracle ILOM 3.0 Quick Start*, modify default network settings
- *Oracle ILOM 3.0 Daily Management Concepts*, network communication settings
- *Oracle ILOM 3.0 Daily Management Concepts*, switch serial port console output
- *Oracle ILOM 3.0 Daily Management CLI Procedures*, configure network settings
- *Oracle ILOM 3.0 Daily Management CLI Procedures*, configure secure shell settings
- *Oracle ILOM 3.0 Daily Management CLI Procedures*, configure serial port sharing
- *Oracle ILOM 3.0 Protocol Management Reference*, configure network settings
- *Oracle ILOM 3.0 Daily Management CLI Procedures*, configure the local interconnect interface

Configuring Network Settings (Web)

Description	Links	Platform Feature Support
Identify requirements for managing Oracle ILOM's network settings	• "Requirements for Network Settings (Web)" on page 22	• x86 system server SP • SPARC system server SP • CMM
Manage and test IPv4 or IPv6 settings	• "View and Configure IPv4 Network Settings (Web)" on page 24 • "View and Configure Dual-Stack IPv4 and IPv6 Network Settings (Web)" on page 25 • "Test IPv4 or IPv6 Network Configuration (Web)" on page 30	• x86 system server SP • SPARC system server SP • CMM
Manage host name, DNS, and serial port settings	• "Assign Host Name and System Identifier (Web)" on page 31 • "View and Configure DNS Settings (Web)" on page 31 • "View and Configure Baud Rate for Serial Port (Web)" on page 32	• x86 system server SP • SPARC system server SP • CMM
Manage serial port sharing settings on x86 hosts	• "Configure x86 Host Serial Port Owner (Web)" on page 33 •	• x86 servers SP
Manage HTTP and HTTPS settings, and upload SSL certificates	• "Enable HTTP or HTTPS Web Access (Web)" on page 34 • "Upload the SSL Certificate (Web)" on page 36	• x86 system server SP • SPARC system server SP • CMM

Requirements for Network Settings (Web)

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

Network Environment	Before You Begin
IPv4-only	• To easily locate Oracle ILOM on the network, you should ensure the same IP address is always assigned to Oracle ILOM. Oracle ILOM by default will attempt to obtain IPv4 network settings using DHCP.
Dual-stack IPv4 and IPv6	• Oracle ILOM is shipped with IPv4 DHCP and IPv6 Stateless default network settings. • Verify that your server or CMM has Oracle ILOM firmware 3.0.12 or later installed. • The IPv4 network state must always be enabled in order for Oracle ILOM to operate in an IPv4 network environment or in a dual-stack IPv4 and IPv6 network environment. • For IPv6 Stateless auto-configurations, Oracle ILOM (3.0.12 or later) requires a network router to be configured for IPv6. • For DHCPv6 auto-configuration options, Oracle 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 Oracle ILOM. For instructions, see "View and Configure DNS Settings (Web)" on page 31. **Note -** For a list of legacy Sun platform servers not supporting IPv6 configurations in Oracle ILOM, refer to Legacy Sun Systems Not Supporting IPv6 in the *Oracle ILOM 3.0 Daily Management Concepts Guide*.
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 (Web)

Before You Begin

- Review the "Requirements for Network Settings (Web)" on page 22.

Note – This procedure provides instructions for configuring Oracle ILOM to operate in an IPv4-only network environment. If you are configuring Oracle ILOM to operate in an dual-stack IPv4 and IPv6 network environment, see "View and Configure Dual-Stack IPv4 and IPv6 Network Settings (Web)" on page 25.

To view and configure IPv4 network settings, follow these steps:

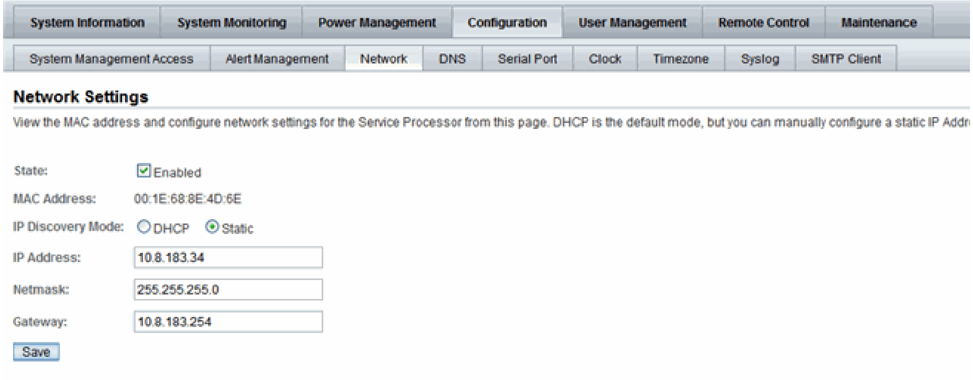
1. **Log in to the Oracle ILOM SP or CMM web interface.**

2. **Click Configuration --> Network.**

   The Network Settings page appears.

3. **You can have DHCP assign IP addresses automatically, or you can choose to assign the addresses manually.**

   - To automatically obtain an IP address, click the radio button next to DHCP. See the following figure.



Network Settings

View the MAC address and configure network settings for the Service Processor from this page. DHCP is the default mode, but you can manually configure a static IP Addr

State: ☑ Enabled

MAC Address: 00:1E:68:8E:4D:6E

IP Discovery Mode: ○ DHCP ● Static

IP Address: 10.8.183.34

Netmask: 255.255.255.0

Gateway: 10.8.183.254

   - To manually set a static IP address, complete the information in the Network Settings page; use the descriptions in the following table.

Item	Description
State	Click the check box to enable the network state.
MAC Address	The SP’s media access control (MAC) address is set at the factory. The MAC address is a hardware address that is unique to each networked device. The MAC address is provided on a label on the SP or CMM, on the Customer Information Sheet included in the ship kit, and in the BIOS Setup screen.
IP Discovery Mode	Click the Static radio button to manually assign an IP address, netmask, and gateway.
IP Address	Type the server’s IP address. The IP address is a unique name that identifies the system on a TCP/IP network.
Netmask	Type the subnet mask of the network on which the SP resides.
Gateway	Type SP’s gateway access address.

4. **Click Save for your settings to take effect.**

   Settings are considered pending until you click Save. Changing the IP address will end your Oracle ILOM session.

   You are prompted to close your web browser.

5. **Log back in to Oracle ILOM using the new IP address.**

Note – If you changed the network settings, you might need to log back in with a new browser session.

▼ View and Configure Dual-Stack IPv4 and IPv6 Network Settings (Web)

Before You Begin

- Review the “Requirements for Network Settings (Web)” on page 22.

Note – This procedure provides instructions for configuring Oracle ILOM to operate in a dual-stack IPv4 and IPv6 network environment. If you are configuring Oracle ILOM to operate in an IPv4-only network environment, refer to “View and Configure IPv4 Network Settings (Web)” on page 24.

To view and configure dual-stack IPv4 and IPv6 network settings, follow these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface.**

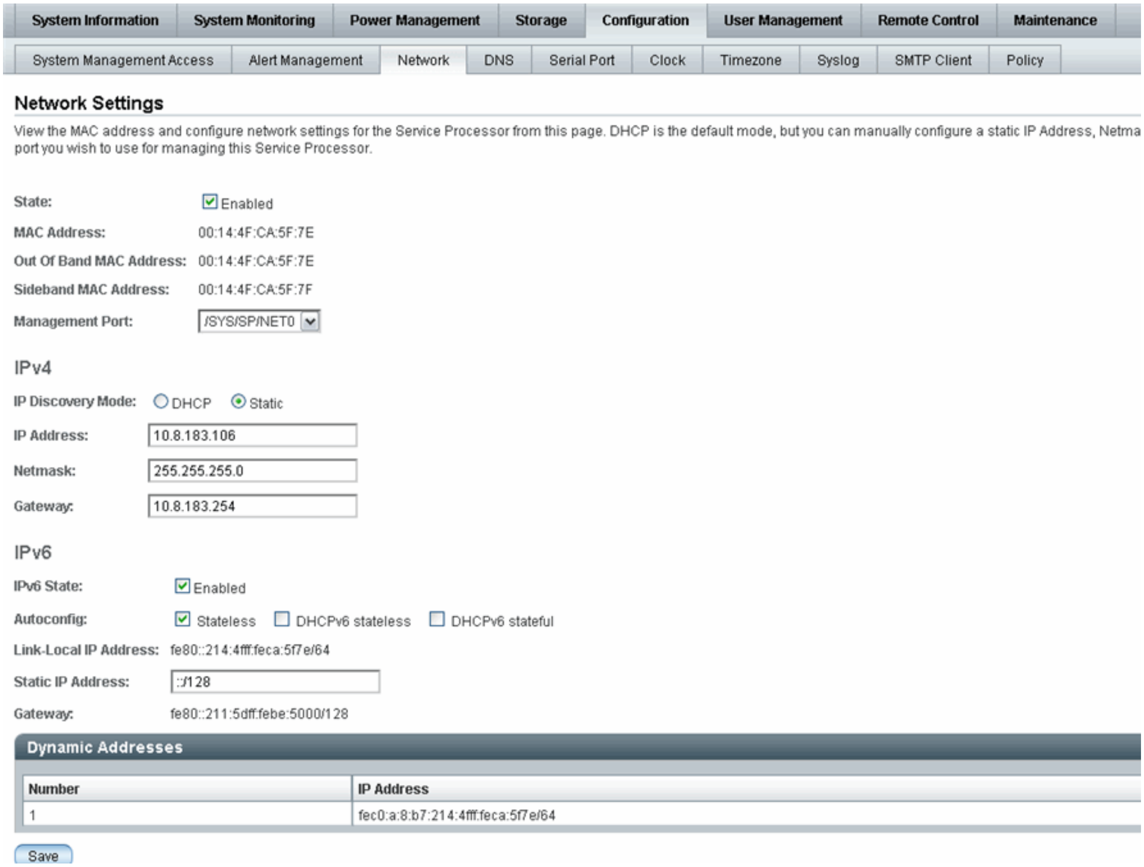
2. **Navigate to the IPv4 and IPv6 network settings that are available on the Network tab.**

   For example:

   - On a server SP, click Configuration --> Network.
   - On a CMM, do the following:
     - Select the blade SP (in the left pane), then (in the right pane) click Configuration --> Network.

Note – The dual-stack IPv4 and IPv6 settings cannot be edited at the CMM level in the Oracle ILOM web interface. To edit the dual-stack IPv4 and IPv6 properties at the CMM level, you must use the Oracle ILOM CLI. For details, see the *Oracle ILOM 3.0 Daily Management – CLI Procedures Guides*.

The following illustration shows the Oracle ILOM SP network settings for IPv4 and IPv6.



Network Settings

View the MAC address and configure network settings for the Service Processor from this page. DHCP is the default mode, but you can manually configure a static IP Address, Netma port you wish to use for managing this Service Processor.

State:	☑ Enabled
MAC Address:	00:14:4F:CA:5F:7E
Out Of Band MAC Address:	00:14:4F:CA:5F:7E
Sideband MAC Address:	00:14:4F:CA:5F:7F
Management Port:	/SYS/SP/NET0

IPv4

IP Discovery Mode:	○ DHCP ● Static
IP Address:	10.8.183.106
Netmask:	255.255.255.0
Gateway:	10.8.183.254

IPv6

IPv6 State:	☑ Enabled
Autoconfig:	☑ Stateless □ DHCPv6 stateless □ DHCPv6 stateful
Link-Local IP Address:	fe80::214:4fff:feca:5f7e/64
Static IP Address:	::/128
Gateway:	fe80::211:5dff:febe:5000/128

Dynamic Addresses

Number	IP Address
1	fec0:a:8:b7:214:4fff:feca:5f7e/64

3. Verify that the network State is enabled.

Note – The network State setting is enabled by default for both IPv4 and IPv6. If necessary, you can optionally disable (unchecked) the network State for IPv6. However, the IPv4 network State must always be enabled in order for Oracle ILOM to operate in an IPv4 network environment or within a dual-stack IPv4 and IPv6 network environment.

---

4. To manually configure a static IPv4 address, perform these steps

Steps	Description
a.	Enable the Static radio button for IPv4.
b.	Type the IP address for the device in the IP address text box.
c.	Type the subnet mask of the network on which the device resides.
d.	Type the device gateway access address.

5. **To enable DHCP to automatically assign an IPv4 address, select the IPv4 DHCP radio button.**

6. **To manually configure a static IPv6 address, type the IP address for the device in the IPv6 address text box.**

   The input parameters for specifying the IPv6 static IP and netmask is:

   <*IPv6_address*>`/<subnet mask length in bits>`

   For example:

   ```
   fec0:a:8:b7:214:4fff:feca:5f7e/64
   ```

Note – IPv6 supports the assignment of multiple IP addresses for a device. Therefore, you can manually configure a single static IPv6 address in Oracle ILOM, as well as enable one or more of the IPv6 auto-configuration options in Oracle ILOM if desired.

---

7. **To enable one or more of the IPv6 auto-configuration options, select the appropriate option(s) described below.**

IPv6 Auto-Configuration Option	Description
Stateless (enabled by default)	When enabled, the Stateless auto-configuration option is run to learn the IPv6 Stateless addresses for the device from the network IPv6 router.
DHCPv6 Stateless	When enabled, the DHCPv6 Stateless auto-configuration option is run to learn the DNS information for the device from the network DHCPv6 server. **Note -** The DHCPv6 Stateless auto-configuration option is available in Oracle ILOM as of 3.0.14.
DHCPv6 Stateful	When enabled, the DHCPv6 Stateful auto-configuration option is run to learn the IPv6 address(es) and DNS information for the device from the network DHCPv6 server. **Note -** The DHCPv6 Stateful auto-configuration option is available in Oracle ILOM as of 3.0.14.

Note – As of Oracle ILOM 3.0.14 or later, you can enable the option for Stateless auto-configuration 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.

Note – When you enable the auto-configuration for either DHCPv6 Stateful or DHCPv6 Stateless, Oracle ILOM will identify in the Network Settings page the DHCP unique ID for the DHCPv6 server that was last used to retrieve the DHCP information.

8. **Click** Save **to apply the changes made.**

   All changes to the network settings are considered pending within the Oracle ILOM session until you click Save.

Note – Changing the static IP address on the device (SP or CMM) will end all active Oracle ILOM sessions to the device. A message will appear prompting you to close your browser session. You will need to log back in to Oracle ILOM using the newly assigned static IP address.

Note – IPv6 addresses learned for the device from any of the IPv6 auto-configuration options will not affect any of the active Oracle ILOM sessions to the device. You can verify the newly learned auto-configured addresses on the Network tab.

9. **To test the IPv4 or IPv6 network configuration from Oracle ILOM, use the Network Test Tools (Ping or Ping6). For details, see** "Test IPv4 or IPv6 Network Configuration (Web)" on page 30**.**

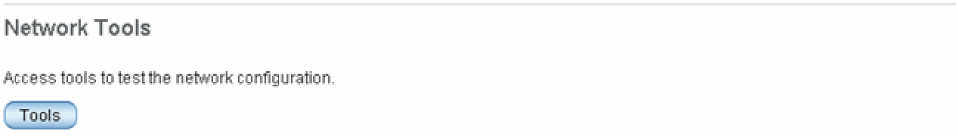
▼ Test IPv4 or IPv6 Network Configuration (Web)

Before You Begin

- Review the "Requirements for Network Settings (Web)" on page 22.

To test the configuration for IPv4 or IPv6, follow these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface.**
2. **In the web interface page, click Configuration --> Network.**
3. **In the Network Settings page, click the Tools button appearing at the bottom of the page.**



Network Tools

Access tools to test the network configuration.

The Test Tools dialog appears.

4. **In the Test Tools dialog, specify the following information:**

Field	Description
Test Type	• Select Ping to test the IPv4 network configuration. or • Select Ping6 to test the IPv6 network configuration.
Destination	Type the IP address of a device on your network (the test is sent to this destination on your network). If the test failed, an error message appears. On some Oracle servers if the test succeeded a succeed message appears.

▼ Assign Host Name and System Identifier (Web)

Before You Begin

- Review the "Requirements for Network Settings (Web)" on page 22.

To assign host name and system identifier, follow these steps:

1. **Log in to the ILOM SP or CMM web interface.**
2. **Click System Information --> Identification Information.**

   The Identification Information page appears.
3. **In the SP host name field, type the SP host name.**

   The host name can contain up to 60 characters.
4. **In the SP System Identifier field, type the text that you will use to identify the system.**

   The system identifier can consist of a text string using any standard keyboard keys except quotation marks.
5. **In the SP System Contact field, type the name of a person you will contact.**

   The system contact can consist of a text string using any standard keyboard keys except quotation marks.
6. **In the SP System Location field, type the text that describes the physical location of the system.**

   The system location can consist of a text string using any standard keyboard keys except quotation marks.
7. **Click Save for your settings to take effect.**

▼ View and Configure DNS Settings (Web)

Before You Begin

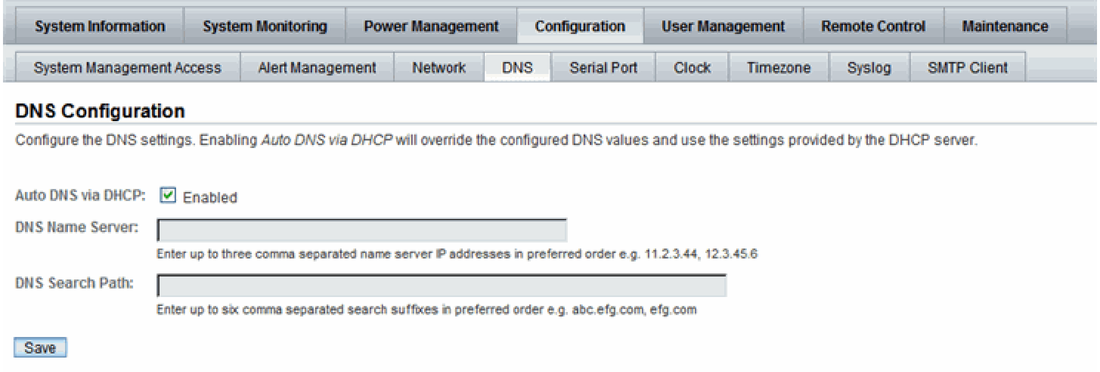
- Review the "Requirements for Network Settings (Web)" on page 22.

To view and configure DNS settings, follow these steps:

1. **Log in to the ILOM SP web interface or the CMM ILOM web interface.**
2. **Click Configuration --> DNS.**

   The DNS Configuration page appears.
3. **You can have DHCP assign the DNS name server and search path automatically, or you can choose to assign the addresses manually.**

- To automatically assign the addresses, enable the checkbox next to Auto DNS via DHCP.
- To manually assign the addresses, complete the DNS name server and DNS search path text boxes. See the following figure.



DNS Configuration

Configure the DNS settings. Enabling *Auto DNS via DHCP* will override the configured DNS values and use the settings provided by the DHCP server.

Auto DNS via DHCP: ☑ Enabled

DNS Name Server:

Enter up to three comma separated name server IP addresses in preferred order e.g. 11.2.3.44, 12.3.45.6

DNS Search Path:

Enter up to six comma separated search suffixes in preferred order e.g. abc.efg.com, efg.com

▼ View and Configure Baud Rate for Serial Port (Web)

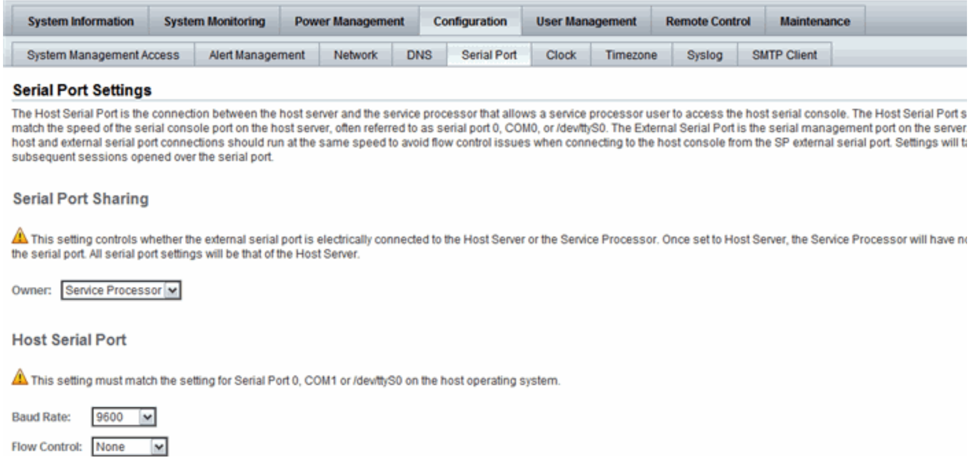
Before You Begin

- Review the "Requirements for Network Settings (Web)" on page 22.

To view and configure serial port baud rate, follow these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface.**
2. **Click Configuration --> Serial Port.**

   The Serial Port Settings page appears.



Serial Port Settings

The Host Serial Port is the connection between the host server and the service processor that allows a service processor user to access the host serial console. The Host Serial Port s match the speed of the serial console port on the host server, often referred to as serial port 0, COM0, or /dev/ttyS0. The External Serial Port is the serial management port on the server host and external serial port connections should run at the same speed to avoid flow control issues when connecting to the host console from the SP external serial port. Settings will t subsequent sessions opened over the serial port.

Serial Port Sharing

⚠ This setting controls whether the external serial port is electrically connected to the Host Server or the Service Processor. Once set to Host Server, the Service Processor will have n the serial port. All serial port settings will be that of the Host Server.

Owner: Service Processor

Host Serial Port

⚠ This setting must match the setting for Serial Port 0, COM1 or /dev/ttyS0 on the host operating system.

Baud Rate: 9600

Flow Control: None

3. **View the baud rate for the internal host serial port and the external serial port.**

4. **From the Host Serial Port Baud Rate drop-down list, select the baud rate for the internal serial port**

   For x64 systems, this setting must match the setting for serial port 0, COM1, or /dev/ttyS0 on the host operating system.

   The baud rate value must match the speed that was specified for the BIOS serial redirection feature (default is 9600 baud) and the speed used for the boot loader and operating system configuration.

   To connect to the system console using Oracle ILOM, you must set the default host serial settings (9600 baud, 8N1 [eight data bits, no parity, one stop bit], no flow control).

5. **From the External Serial Port Baud Rate drop-down list, select the baud rate for the external serial port.**

   This setting must match the baud rate on the RJ-45 serial port on the Oracle Sun server.

6. **Click Save for your changes to take effect.**

▼ Configure x86 Host Serial Port Owner (Web)

Before You Begin

- Review the "Requirements for Network Settings (Web)" on page 22.

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

Caution – You should set up a network management connection to the SP before attempting to switch the serial port owner to the host server. If a network management connection is not set up to the server SP, and the serial port owner was changed from the SP to the host server, you will not be able to use the ILOM CLI or web interface to return the SP as the serial port owner. In order to return the serial port owner to the SP, you will need to restore access to ILOM through the serial management port on the server. For more details about accessing ILOM through the serial management (SER MGT) port on your server, see the platform documentation supplied with your server.

To configure the host serial port owner on an x86 platform server, follow these steps:

1. **Log in to the Oracle ILOM SP web interface.**
2. **Select the Configuration --> Serial Port.**

   The Serial Port Settings page appears.
3. **In the Serial Port Settings page, select** `Host Server` **as the serial port owner.**

Note – The service processor is the default serial port owner property value.

4. **Click Save for the changes to take effect.**

Note – Changing the "serial port owner" and saving this change might result in the following benign error: `Can not change serial settings - the serial console in use.` This error occurs if there is an active session on the serial port. However, changes to the port owner, as well as any changes to the port speed will take affect in Oracle ILOM.

5. **Connect a serial host to the server.**

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

▼ Enable HTTP or HTTPS Web Access (Web)

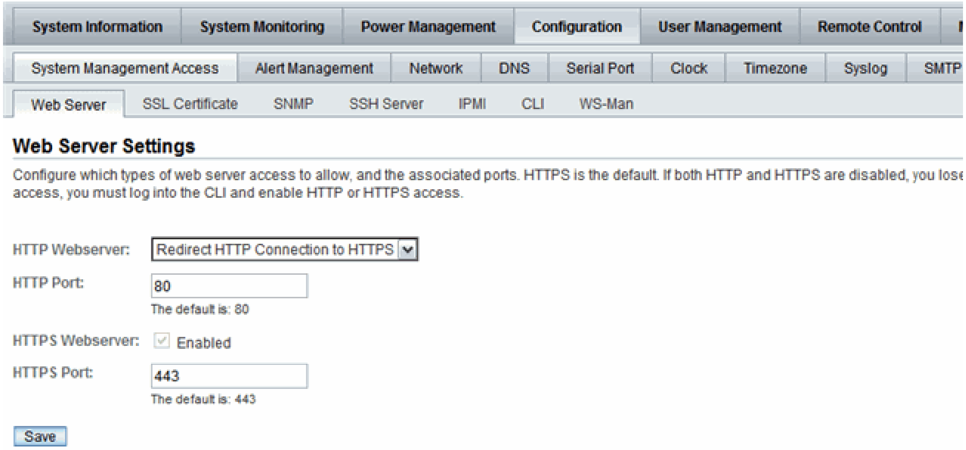
Before You Begin

- Review the “Requirements for Network Settings (Web)” on page 22.

To enable HTTP or HTTPS web access, follow these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface.**
2. **Click Configuration --> System Management Access --> Web Server.**

   The Web Server Settings page appears.



Web Server Settings

Configure which types of web server access to allow, and the associated ports. HTTPS is the default. If both HTTP and HTTPS are disabled, you lose access, you must log into the CLI and enable HTTP or HTTPS access.

HTTP Webserver: Redirect HTTP Connection to HTTPS

HTTP Port: 80

The default is: 80

HTTPS Webserver: ☑ Enabled

HTTPS Port: 443

The default is: 443

3. **Perform one of the following:**
   - To enable HTTP, select Enabled from the HTTP Webserver: drop-down list.
   - To automatically redirect HTTP connections to HTTPS, select Redirect HTTP Connection to HTTPS from the HTTP Webserver: drop-down list
   - To disable HTTP, select Disabled from the HTTP Webserver: drop-down list
   - To enable HTTPS, select the checkbox for HTTPS Web Server Enabled.

     The HTTPS web server is enabled by default.

Note – If you disable HTTP or select Redirect HTTP Connection to HTTPS, and then disable HTTPS, you will be unable to access the Oracle ILOM web interface. To restore access, use the CLI `/SP/services/http` or `/SP/services/https` commands, as described in “Enable HTTP or HTTPS Web Access“ in the *Oracle ILOM 3.0 CLI Procedures Guide*.

---

4. **Assign an HTTP or HTTPS port number.**
5. **Click Save.**

▼ Upload the SSL Certificate (Web)

Before You Begin

- Review the "Requirements for Network Settings (Web)" on page 22.
- Oracle ILOM does not apply changes to the SSL certificate and key until both the SSL Certificate and key have been uploaded.

Note – Oracle ILOM provides a default SSL certificate and self-signed key for HTTPS access. Optionally, you can upload a different SSL certificate and matching private key. Ensure that you can access the new certificate and key through your network or local file system.

To upload the SSL certificate, follow these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface**

2. **Click Configuration --> System Management Access --> SSL Certificate.**

   The SSL Certificate Upload page appears.

3. **Type the file name of the new SSL certificate or click the Browse button to search for a new SSL certificate.**

   The file name has a `.pem` file extension. The service processor does not support pass-phrase-encrypted certificates.

4. **Click the Upload button to obtain the selected SSL certificate.**

   The SSL Certificate Upload Status dialog box appears.

5. **After you have uploaded the certificate and private key, click the OK button to reset the Oracle ILOM web server and begin using the new SSL certificate.**

   The Oracle ILOM web server must be reset for the new certificate to take effect.

Configuring Secure Shell Settings

Description	Links	Platform Feature Support
Manage Secure Shell settings	• "Enable or Disable SSH" on page 37 • "Generate a New SSH Key" on page 37 • "Restart the SSH Server" on page 38	• x86 system server SP • SPARC system server SP • CMM

▼ Enable or Disable SSH

Before You Begin

Note – SSH is enabled by default in Oracle ILOM.

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

To enable or disable SSH, follow these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface**
2. **Click Configuration --> System Management Access --> SSH Server.**

   The SSH Server Settings page appears.
3. **To enable the SSH server, click the Enabled check box next to State.**
4. **Click Save for your settings to take effect.**

▼ Generate a New SSH Key

Before You Begin

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

To generate a new SSH Key, follow these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface**

2. **Click Configuration --> System Management Access --> SSH Server.**

   The SSH Server Settings page appears.

3. **Select RSA by clicking the Generate RSA Key button, or select DSA by clicking the Generate DSA Key button.**

   Click OK or Cancel when you are prompted.

   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.

To restart the SSH server, follow these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface.**
2. **Click Configuration --> System Management Access --> SSH Server.**

   The SSH Server Settings page appears.

3. **Click the Restart button to restart the SSH server.**

Configuring the Local Interconnect Interface (Web)

Description	Links	Platform Feature Support
Identify requirements for configuring the local interconnect interface	• "Requirements for Configure Local Interconnect" on page 39	• x86 system server SP • SPARC system server SP
Configure the Local Interconnect Interface	• "Configure the Local Interconnect Interface (Web)" on page 40	

Requirements for Configure Local Interconnect

The following requirements must be met before you perform the procedures described in this section.

- Review the concepts describing the use of a Local Interconnect Interface between the Oracle ILOM SP and the host OS. For details, refer to "Local Interconnect Interface: Local Connection to Oracle ILOM From Host " in the *Oracle ILOM 3.0 Daily Management Concepts Guide*.
- Review the Oracle ILOM descriptions for the Local Host Interconnect configuration settings. For details, refer to "Local Host Interconnect Configuration Settings in Oracle ILOM" in the *Oracle ILOM 3.0 Daily Management Concepts Guide*.
- Verify that your server is running Oracle ILOM 3.0.12 or a later version of Oracle ILOM.
- Verify that your platform supports the Local Interconnect Interface. Refer to your platform server Oracle ILOM supplement guide or administration guide.

Note – The settings in Oracle 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 Oracle 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, refer to the *Oracle Server Hardware Management Pack User's Guide*.
- Manual configuration of the Local Interconnect Interface between the Oracle ILOM SP and the host operating system requires the Host Managed (`hostmanaged`) setting in Oracle 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 147.
- The host operating system must support the internal USB Ethernet device that is presented from the Oracle ILOM SP. Therefore, prior to configuring the Local Interconnect Interface in Oracle 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, refer to the *Oracle Server Hardware Management Pack User's Guide*.

- Network parameter changes to the settings in Oracle ILOM for the Local Interconnect Interface are considered pending until you commit the changes in the Oracle ILOM. For example, in the Oracle ILOM CLI, you must issue the `commitpending=true` command to save the `pendingipaddress` and the `pendingipnetmask` under the `network/interconnect` target. In the Oracle ILOM web interface, network parameter changes entered on the Configure USB Ethernet Parameters dialog box are committed after you click `Save`.
- An Oracle ILOM user account with Admin (`a`) role privileges is required in order to change any of the settings in Oracle 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.

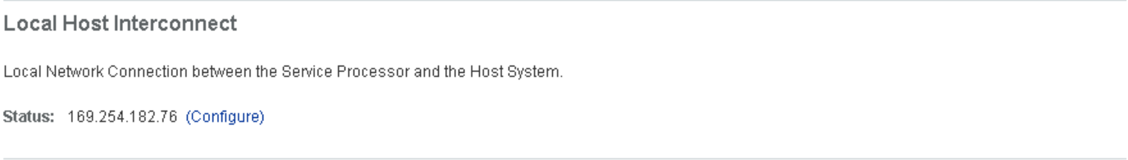
▼ Configure the Local Interconnect Interface (Web)

Before You Begin

- Review the "Requirements for Configure Local Interconnect" on page 39

To configure the local interconnect interface using the Oracle ILOM web interface, follow these steps:

1. **Log in to the Oracle ILOM SP web interface.**
2. **In the web interface page, click Configuration --> Network.**
3. **In the Network Settings page, scroll down the page until you see the section labeled "Local Host Interconnect," then click Configure.**

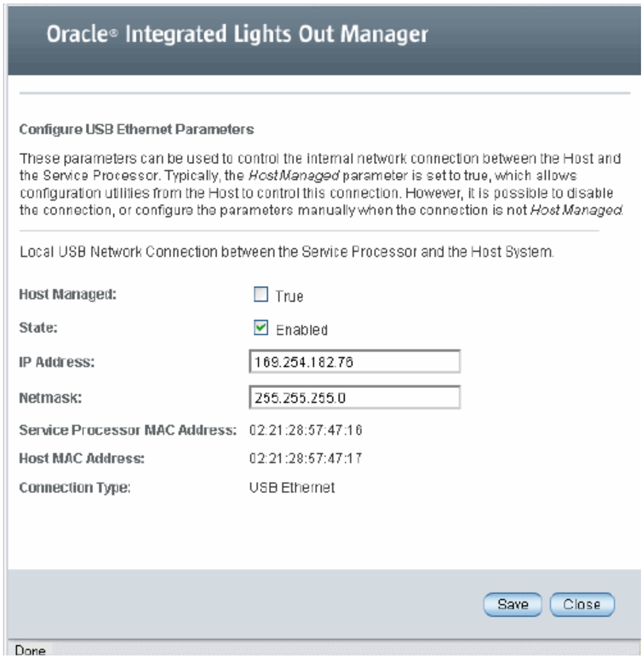


Local Host Interconnect

Local Network Connection between the Service Processor and the Host System.

Status: 169.254.182.76 (Configure)

The dialog box to configure the USB Ethernet Parameters appears.



Oracle® Integrated Lights Out Manager

Configure USB Ethernet Parameters

These parameters can be used to control the internal network connection between the Host and the Service Processor. Typically, the *Host Managed* parameter is set to true, which allows configuration utilities from the Host to control this connection. However, it is possible to disable the connection, or configure the parameters manually when the connection is not *Host Managed*.

Local USB Network Connection between the Service Processor and the Host System.

Host Managed:	□ True
State:	☑ Enabled
IP Address:	169.254.182.76
Netmask:	255.255.255.0
Service Processor MAC Address:	02:21:28:57:47:16
Host MAC Address:	02:21:28:57:47:17
Connection Type:	USB Ethernet

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 enabling the check box for True Host Management.
   - When you enable the Host Managed property setting, you also must install the Oracle Hardware Management Pack 2.1.0 (or later) software on your server and accept the installation default for enabling Local Oracle ILOM Interconnect. For more information, refer to the section about configuring the Local Oracle ILOM Interconnect in the *Oracle Server Hardware Management Pack User's Guide*
   - Manually assign non-routable IPv4 addresses to each connection point on the Local Interconnect Interface by specifying the following properties in the Configure USB Ethernet Parameters dialog:

Field	Instructions and Description
Host Managed	Clear the check box for Host Managed to disable the host managed mode.
State	Click the check box for `State` to manually enable the local interconnect mode between the Oracle ILOM SP and the host OS. The `State` is, by default, disabled.
IP Address	Oracle ILOM, by default, provides a default non-routable IPv4 address for the Oracle 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 in your network environment with this IPv4 address.
NetMask	Oracle ILOM, by default, provides a default IPv4 Netmask address for the Oracle 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.

Note – To prevent the Oracle Hardware Management Pack software from auto-configuring the Local Interconnect Interface between the Oracle ILOM SP and the host OS, the Host Managed must be cleared (disabled). To prevent the use of the Local Interconnect Interface between the Oracle ILOM SP and the host OS, both the Host Managed check box and the State check box must be cleared (disabled).

5. **To commit the changes entered on the Configure USB Ethernet Parameters dialog box, click Save.**

Note – If you chose to manually configure the Local Interconnect Interface in Oracle ILOM without the use of the Oracle Hardware Management Pack 2.1.0 or later 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 147.

Managing User Accounts (Web)

Description	Links
Configure user accounts	• "Configuring User Accounts (Web)" on page 44
Configure SSH user key	• "Configuring SSH Keys (Web)" on page 50
Configure Active Directory settings	• "Configuring Active Directory (Web)" on page 53
Configure LDAP settings	• "Configuring Lightweight Directory Access Protocol (LDAP)" on page 63
Configure LDAP/SSL settings	• "Configuring LDAP/SSL Settings (Web)" on page 65
Configure RADIUS settings	• "Configuring RADIUS (Web)" on page 73

Related Information

- Oracle ILOM 3.0 Quick Start, add user account
- *Oracle ILOM 3.0 Daily Management Concepts*, user account management
- *Oracle ILOM 3.0 Daily Management Concepts*, guidelines for managing user accounts
- *Oracle ILOM 3.0 Daily Management CLI Procedures*, recover a lost password
- *Oracle ILOM 3.0 Daily Management CLI Procedures*, manage user accounts
- *Oracle ILOM 3.0 Protocol Management Reference*, manage user accounts

Configuring User Accounts (Web)

Description	Links	Platform Feature Support
Manage Oracle ILOM's single sign on and user session settings	• "Configure Single Sign On (Web)" on page 44 • "Set the Session Time-Out (Web)" on page 45	• x86 system server SP • SPARC system server SP • CMM
Manage Oracle ILOM user accounts and roles	• "Add User Accounts and Assign Roles (Web)" on page 45 • "Modify a User Account (Web)" on page 48 • "Delete a User Account (Web)" on page 49 • "View User Sessions (Web)" on page 50	• x86 system server SP • SPARC system server SP • CMM

▼ Configure Single Sign On (Web)

Before You Begin

- To set properties for Single Sign On, you need the Admin (a) role enabled.

To enable or disable single sign on, follow these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface.**
2. **Click User Management --> User Accounts.**

   The User Account Settings page appears.
3. **Click the check box next to Enable Single Sign On to enable the feature, or clear the check box to disable the feature.**

▼ Set the Session Time-Out (Web)

Note – The session time-out setting controls the amount of time an Oracle ILOM session will remain idle before logging out. The session time-out setting does not persist after you log out of the current Oracle ILOM session. You must reset the session time-out each time you log in to the Oracle ILOM web interface.

Before You Begin

- To set properties for session time-out, you need the Admin (a) role enabled.

To set the session time-out property value, follow these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface.**
2. **Click System Information --> Session Time-Out.**

   The Session Time-Out page appears.
3. **In the Session Time-Out drop-down list, select a preferred time-out increment (15 mins, 30 mins, 1 hr, or 3 hrs).**
4. **Click Apply to save your changes.**

▼ Add User Accounts and Assign Roles (Web)

Before You Begin

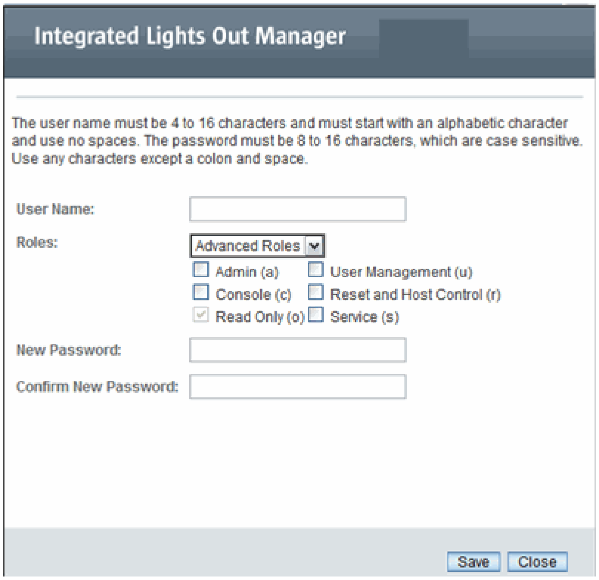
- To set properties for User Management (user accounts and roles), you need the User Management (u) role enabled.

To add a user account and assign privileges (roles), follow these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface.**
2. **Click User Management --> User Accounts.**

   The User Account Settings page appears.
3. **In the Users table, click Add.**

   The Add User dialog box appears.


Integrated Lights Out Manager

The user name must be 4 to 16 characters and must start with an alphabetic character and use no spaces. The password must be 8 to 16 characters, which are case sensitive. Use any characters except a colon and space.

User Name:

Roles: Advanced Roles

□ Admin (a) □ User Management (u)
□ Console (c) □ Reset and Host Control (r)
☑ Read Only (o) □ Service (s)

New Password:

Confirm New Password:

4. **Complete the following information:**

   a. **In the User Name text box, specify a name for this user account.**

   b. **In the Roles drop-down list, select a user role profile (administrator, operator, or advanced).**

      User role profile descriptions follow.

User Role Descriptions

User role profiles	User role profile permissions granted (web)
Administrator	When selected, the Administrator role profile in the Oracle ILOM web interface automatically grants read and write permissions to the following user role permissions. • Admin (a) • User Management (u) • Console (c) • Reset and Host Control (r) • Read only (o) For definitions of roles supported by the Administrator role profile, see the user role definitions listed in this table under **User role permissions granted**.

User Role Descriptions	
Operator	When selected, the Operator role profile in the Oracle ILOM web interface automatically grants the following user role permissions: • Console (c) • Reset and Host Control (r) • Read only (o) For definitions of roles granted by the Operator role profile, see the user role definitions listed in this table under **User role permissions granted**.
Advanced	When selected, the Advanced role profile in the Oracle ILOM web interface automatically grants Read Only (o) permissions to all Oracle functions and enables you to assign all or any combination of the following role permissions of interest: • Admin (a) • User Management (u) • Console (c) • Reset and Host Control (r). • Services (s) For definitions of roles granted by the Advanced role profile, see the user role definitions listed in this table under **User role permissions granted**.
User roles	**User role permissions granted (CLI)**
(a)	Admin (a). Read and write permissions are granted to all Oracle ILOM system management functions with the exception of the functions that would require the Admin to have these additional user roles enabled: User Management (u), Reset and Host Control (r), Console (c), and Services (s).
(u)	User Management (u). Read and write permissions are granted to a user for all Oracle ILOM user account management functions.
(c)	Console (c). Read and write permissions are granted to a user to perform these Remote Console management functions: manage Remote Console lock options, manage SP console history log options, launch and use Oracle ILOM Remote Console, and launch and use Oracle ILOM Storage Redirection CLI.
(r)	Reset and Host Control (r). Read and write permissions are granted to a user to perform these remote host management functions: host boot device control, run and configure diagnostics utilities, reset SP, reset CMM, component management service actions, fault management actions, SPARC TPM management actions, and downloads of SNMP MIBs.
(o)	Read Only (o). Read only permissions are granted to a user to view the state of all ILOM configuration properties. In addition, write permissions are granted to a user to change only the password and session time-out properties assigned to their own user account.
(s)	Services (s). Read and write permissions are granted to a user to assist Oracle service engineers if on-site service is required.

User Role	Descriptions
(aucro)	A combination of all these users roles (aucro) grant read and write permissions to a user to perform backup and restore configuration functions. **Note -** `aucro` is equivalent to the Administrator user role profile in the web interface.

c. **In the New Password text box, type a password for this user account.**

The password must be at least 8 characters and no more than 16 characters. The password is case-sensitive. Use alphabetical, numeric, and special characters for better security. You can use any character except a colon. Do not include spaces in passwords.

d. **In the Confirm Password text box, retype the password previously entered in the New Password text box.**

e. **Click Save to create the user account.**

The User Account Settings page refreshes. The newly created user account appears on the User Account Settings page.

▼ Modify a User Account (Web)

Note – You can modify a user account by changing the user's password, and the user's network and serial privileges.

Before You Begin

- To set properties for User Management (user accounts and roles), you need the User Management (u) role enabled.

To modify a user account, follow these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface.**

2. **Click User Management --> User Accounts.**

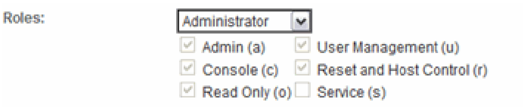
   The User Account Settings page appears.

3. **In the Users table, enable the radio button next to the user account you want to modify and click Edit.**

   A dialog box appears listing the role assigned.

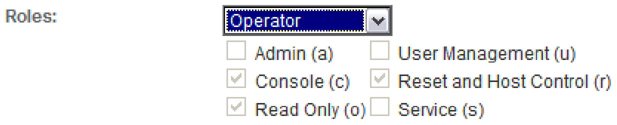
4. **Modify the role assigned to a user.**

   Note that when the Advanced role is selected, a user can select any of the six available roles. However, if you selected Administrator or Operator, Oracle ILOM will automatically assign the roles. For example, the two following figures identify the roles assigned by Oracle ILOM for Administrator and Operator.



Roles: Administrator

☑ Admin (a) ☑ User Management (u)
☑ Console (c) ☑ Reset and Host Control (r)
☑ Read Only (o) □ Service (s)



Roles: Operator

□ Admin (a) □ User Management (u)
☑ Console (c) ☑ Reset and Host Control (r)
☑ Read Only (o) □ Service (s)

5. **In the New Password text box, specify a new password for this user account.**

   The password must be between 8 and 16 characters. The password is case-sensitive. Use alphabetical, numeric, and special characters for better security. You can use any character except a colon. Do not include spaces in passwords.

6. **In the Confirm New Password text, retype the password previously entered in the New Password text box.**

7. **Click Save for the changes to take effect, or click Close to return to the previous settings.**

   The User Account Settings page refreshes with your changes.

▼ Delete a User Account (Web)

Before You Begin

- To set properties for User Management (user accounts and roles), you need the User Management (u) role enabled.

To delete a user account, follow these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface.**

2. **Click User Management --> User Accounts.**

   The User Account Settings page appears.

3. **Enable the radio button next to the user account you want to delete.**

4. **In the Users table, click Delete.**

   A confirmation dialog box appears.

5. **Click OK to delete the account or click Cancel to stop the deletion process.**

   The User Account Settings page refreshes.

▼ View User Sessions (Web)

1. **Log in to the Oracle ILOM SP or CMM web interface.**
2. **Click User Management --> Active Sessions.**

   The Active Sessions page appears listing the name of the user account, user role assigned, session start-time, session type, and the session mode.

Configuring SSH Keys (Web)

Description	Links	Platform Feature Support
Manage SSH key settings in the Oracle ILOM web interface	• "Add an SSH Key (Web)" on page 50 • "Delete an SSH Key (Web)" on page 52	• x86 system server SP • SPARC system server SP • CMM

▼ Add an SSH Key (Web)

Note – The SSH key settings in Oracle ILOM enable you to automate password authentication.

Before You Begin

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

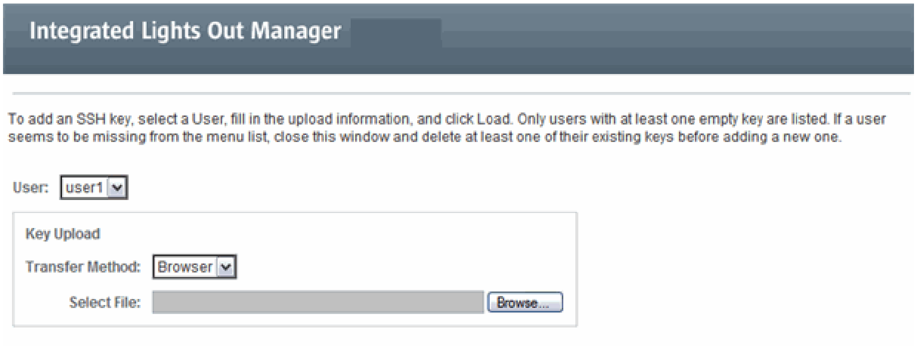
To add an SSH key, follow these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface.**
2. **Click User Management --> User Accounts.**

   The User Accounts Setting page appears.

3. **In the User Account Settings page, scroll down to the SSH table and click Add.**

   The SSH key add screen appears.



Integrated Lights Out Manager

To add an SSH key, select a User, fill in the upload information, and click Load. Only users with at least one empty key are listed. If a user seems to be missing from the menu list, close this window and delete at least one of their existing keys before adding a new one.

User: user1

Key Upload

Transfer Method: Browser

Select File:

4. **In the User drop-down list, select the name of the user account.**

5. **In the Transfer Method drop-down list, select a transfer method.**

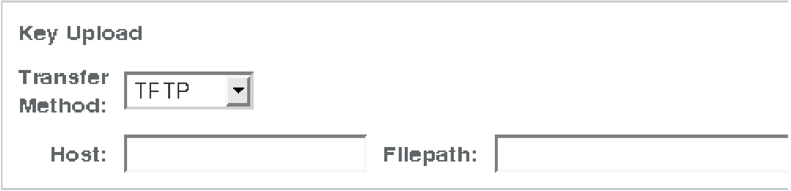
   The following transfer methods are available:

   - Browser
   - TFTP
   - FTP
   - SFTP
   - SCP
   - HTTP
   - HTTPS

6. **If you select the Browser transfer method, click Browse and browse to the location of the SSH key. Proceed to Step 9.**

7. **If you select the TFTP transfer method, the prompts shown in the following figure appear and you must provide the following information, then proceed to Step 9:**

   - **Host** – Enter the remote host IP address or, if you have DNS configured, the name of the remote host.
   - **Filepath** – Enter the path to which to save the configuration file in the format: `directoryPath/filename`.



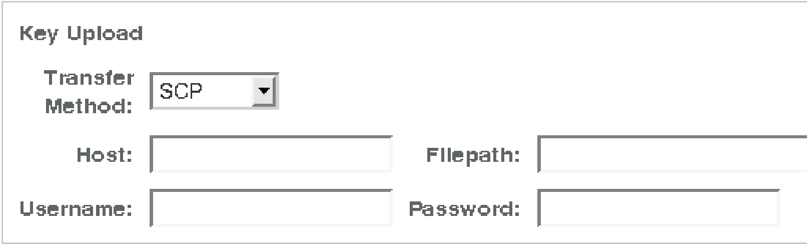
Key Upload

Transfer Method: TFTP

Host:

Filepath:

8. **If you select the SCP, FTP, SFTP, HTTP, or HTTPS transfer method, the prompts shown in the next figure, appear and you must provide the following information, then proceed to Step 9:**
   - **Host** – Enter the remote host IP address or, if you have DNS configured, the name of the remote host.
   - **Filepath** – Enter the path to which to save the configuration file in the format: `directoryPath/filename`.
   - **Username** – Enter the user name of your account on the remote system.
   - **Password** – Enter the password for your account on the remote system.



Key Upload

Transfer Method: SCP

Host:

Filepath:

Username:

Password:

9. **To add the SSH key to the selected user account, click Load.**

   The SSH key is added to the user account.

▼ Delete an SSH Key (Web)

Note – The SSH key settings in Oracle ILOM enable you to automate password authentication.

Before You Begin

- To change other user SSH Keys, you need the User Management (u) role enabled. However, you can configure your own SSH Key with the Read Only (o) role enabled.

To delete an SSH key, follow these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface.**
2. **Click User Management--> User Accounts.**

   The User Account Settings page appears.
3. **Scroll down to the SSH keys section at the bottom of the page, select a user, and click Delete.**

   A confirmation dialog box appears.
4. **Click OK.**

   The SSH key is deleted.

Configuring Active Directory (Web)

Description	Links	Platform Feature Support
Manage and troubleshoot Active Directory settings in the Oracle ILOM web interface	• "View and Configure Active Directory Settings (Web)" on page 53 • "Configure Active Directory Groups (Web)" on page 58 • "Troubleshoot Active Directory Authentication and Authorization (Web)" on page 61	• x86 system server SP • SPARC system server SP • CMM

▼ View and Configure Active Directory Settings (Web)

Before You Begin

- To configure Active Directory settings, you need the User Management (u) role enabled.
- To configure the Expanded Search Mode property, the server or CMM must be running Oracle ILOM firmware version 3.0.4 or later.
- To configure the Strict Credential Error Mode property, the server or CMM must be running Oracle ILOM firmware version 3.0.10 or later.

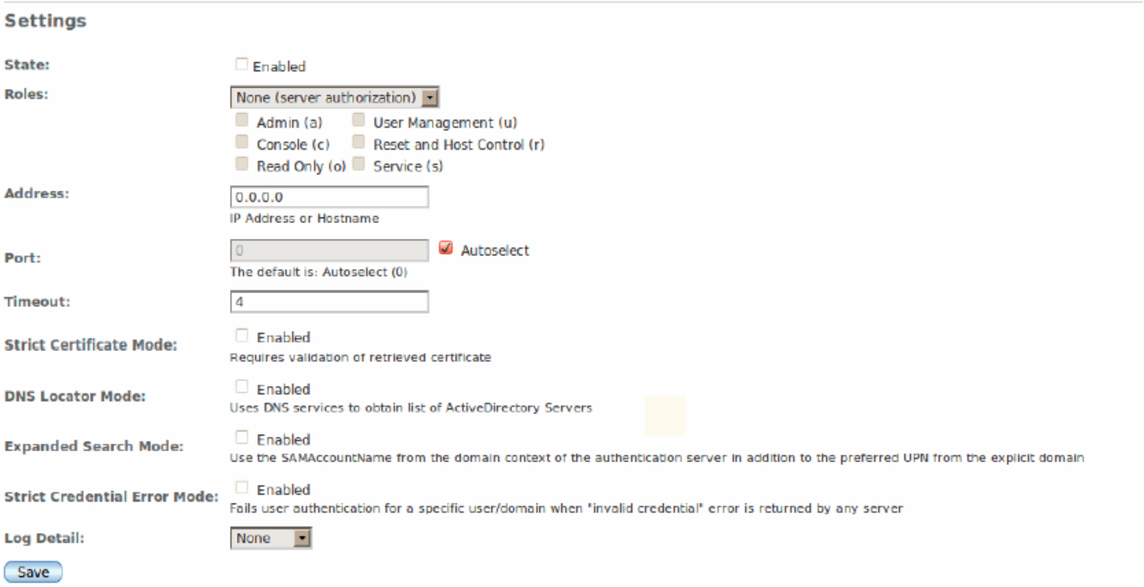
To view and configure Active Directory settings, follow these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface.**

2. **Click User Management --> Active Directory.**

   The Active Directory page appears. There are three sections to the Active Directory page, as shown in the following figures.

   - The top section, which includes targets and properties:



Settings

State: □ Enabled

Roles: None (server authorization)
□ Admin (a) □ User Management (u)
□ Console (c) □ Reset and Host Control (r)
□ Read Only (o) □ Service (s)

Address: 0.0.0.0
IP Address or Hostname

Port: 0 ☑ Autoselect
The default is: Autoselect (0)

Timeout: 4

Strict Certificate Mode: □ Enabled
Requires validation of retrieved certificate

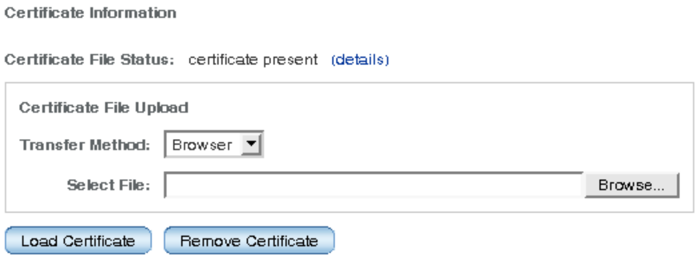
DNS Locator Mode: □ Enabled
Uses DNS services to obtain list of ActiveDirectory Servers

Expanded Search Mode: □ Enabled
Use the SAMAccountName from the domain context of the authentication server in addition to the preferred UPN from the explicit domain

Strict Credential Error Mode: □ Enabled
Fails user authentication for a specific user/domain when "invalid credential" error is returned by any server

Log Detail: None

   - The middle section, which includes the primary certificate information:



Certificate Information

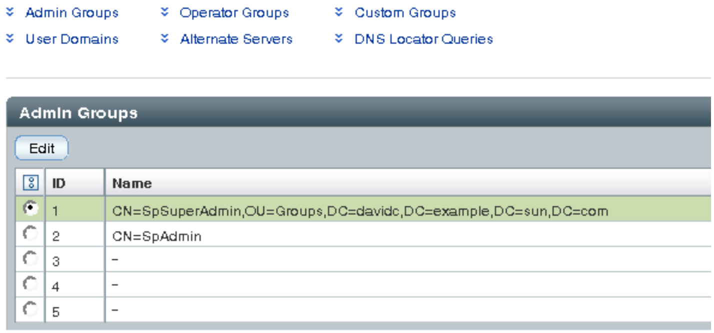
Certificate File Status: certificate present (details)

Certificate File Upload

Transfer Method: Browser

Select File:

   - The bottom section, which includes the Active Directory tables:



Admin Groups · Operator Groups · Custom Groups

User Domains · Alternate Servers · DNS Locator Queries

Admin Groups

Edit

	ID	Name
●	1	CN=SpSuperAdmin,OU=Groups,DC=davidc,DC=example,DC=sun,DC=com
○	2	CN=SpAdmin
○	3	-
○	4	-
○	5	-

3. **Configure the Active Directory settings appearing in the top section of the Active Directory Settings page.**

   See the following table for a description of the Active Directory settings.

Property	Default	Description
State	Disabled	Enabled | Disabled
Roles	(none)	Administrator | Operator | Advanced | none Access role granted to all authenticated Active Directory 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, o=Read-Only, and s=Service. If you do not configure a role, the Active Directory server is used to determine the role.
Address	0.0.0.0	IP address or DNS name of the Active Directory server. If DNS name is used, then DNS must be configured and operational.
Port	0	Port used to communicate with the server. If autoselect is selected, the port is set to 0. Available in the unlikely event of a non-standard TCP port being used.
Timeout	4	Time-out value in seconds. Number of seconds to wait for individual transactions to complete. The value does not represent the total time of all transactions because the number of transactions can differ depending on the configuration. This property allows for tuning the time to wait when a server is not responding or is unreachable.

Property	Default	Description
Strict Certificate Mode	Disabled	Enabled | Disabled If enabled, the server certificate contents are verified by digital signatures at the time of authentication. Certificate must be loaded before Strict Certificate Mode can be set to enabled.
DNS Locator Mode	Disabled	Enabled | Disabled If enabled, an attempt to locate the Active Directory server is performed, based on the DNS locator queries that are configured.
Expanded Search Mode	Disabled	Enabled | Disabled As of Oracle ILOM 3.0.4, an expanded search mode is available. When enabled, you can use the expanded search mode to control the search for user entries. Different searches are attempted if the more specific userPrincipleName search does not immediately succeed. If disabled, the userPrincipleName is expected to have a fully qualified domain name (FQDN) suffix.
Strict Credential Error Mode	Disabled	Enabled | Disabled As of Oracle ILOM 3.0.10, the Strict Credential Error Mode is available. If the mode is set to disabled (cleared check box), user-credential errors are retried on other servers that are available (either configured through the alternate server table or found by DNS queries). The disabled state allows users from separate, disjoint domains to log in to Oracle ILOM as long as that domain authentication server is available. If the mode is set to enabled (checked check box), a credential error reported from any server fails those user credentials after the first authentication attempt showing the user-credential error.
Log Detail	None	None | High | Medium | Low Specifies the amount of diagnostics that go into the event log.

4. **Click Save in the top section of the Active Directory settings page for your settings to take effect.**

5. **View the Active Directory certificate information in the middle section of the Active Directory settings page.**

   See the following table for a description of Active Directory certificate settings.

Property	Displays	Description
Certificate File Status	Certificate not present	Read-only indicator of whether a certificate exists.
Certificate File Status	Certificate present (details)	Click the (details) link to view certificate information about issuer, subject, serial number, valid from, valid to, and version.

6. **If Strict Certificate Mode is enabled, perform the following steps:**

Note – If Strict Certificate Mode is disabled, data will continue to be protected but a certificate is not required to be uploaded.

   a. **Complete the "Certificate File Upload" section by specifying the required parameters to upload the certificate file.**

Transfer Method	Required Parameters
Browser	File Name
TFTP	Host Filepath
FTP	Host Filepath Username Password
SCP	Host Filepath Username Password

   b. **Click the Load Certificate button.**

   c. **When the certificate is loaded, click the "details" link to show the following information.**

Item	Description
Issuer	Certificate Authority who issued the certificate.
Subject	Server or domain for which the certificate is intended.

Valid From	Date when the certificate becomes valid.
Valid Until	Date when the certificate becomes invalid.
`Serial Number`	Serial number of the certificate.
Version	Version number of the certificate.

▼ Configure Active Directory Groups (Web)

Before You Begin

- To configure Active Directory settings, you need the User Management (u) role enabled.
- To configure the Expanded Search Mode property, the server or CMM must be running Oracle ILOM firmware version 3.0.4 or later.
- To configure the Strict Credential Error Mode property, the server or CMM must be running Oracle ILOM firmware version 3.0.10 or later.

To configure Active Directory tables, follow these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface.**
2. **Click User Management --> Active Directory.**

   The Active Directory page appears.
3. **At the top of the Active Directory page, click the link to access the category of table you want to configure:**
   - Admin Groups
   - Operator Groups
   - Custom Groups
   - User Domains
   - Alternate Servers
   - DNS Locator Queries
4. **Enable the radio button of the individual table, and then click Edit.**
5. **Enter the required data into the tables.**

   In the following tables, default data shows the expected format of the Active Directory data.
   - **Admin Groups table:**

     Use the Admin Groups table to view and configure properties for one or more Microsoft Active Directory Admin Groups. Supported formats for configuring Admin Groups include:

Note – The name field supports up to 128 characters. If the chosen format is over 128 characters, you should use one of the other supported formats with fewer characters.

- **Distinguished Name (DN) Format** – `CN=admingroup,OU=Groups,DC=domain,DC=company,DC=com`.

  For example:

  `CN=SpSuperAdmin,OU=Groups,DC=sales,DC=east,DC=oracle,DC=com`
- **Simple Name Format** – admingroup
- **NT-Style Name** – domain\admingroup
- **Domain Format** – DC=domain,DC=company,DC=com\admingroup

- **Operator Groups table:**

  Use the Operator Groups table to view and configure the Microsoft Active Directory Operator groups. Supported formats for configuring operator groups include: Distinguished Name (DN) format, Simple Name format, or NT-Style Name.

  `CN=SpSuperOper,OU=Groups,DC=sales,DC=east,DC=oracle,DC=com`
- **Custom Groups table**:

  Use the Custom Groups table to view and configure properties for one or more Microsoft Active Directory custom groups . Supported formats for configuring custom groups include: Distinguished Name (DN) format, Simple Name format, or NT-Style Name.

  `Example Gustom Group Name: custom_group_1`

  Configurable User Roles: `Admin, User Management, Console, Reset and Host Control, Read Only (aucro)`
- **User Domains table:**

  Use the User Domain table to view and configure properties for one or more Microsoft Active Directory User Domains.

  User domains are the authentication domains used to authenticate a user. When the user logs in, the name used is formatted in the specific domain name format. User authentication is attempted based on the user name that is entered and the configured user domains.

  For example:

  - The principle format used in the first attempt to authenticate the user

    <*USERNAME*>@sales.east.oracle.com
  - The Distinguished Name format is used if the first attempt to authenticate the user failed.

CN=<USERNAME>,CN=Users,DC=sales,DC=east,DC=oracle,DC=com

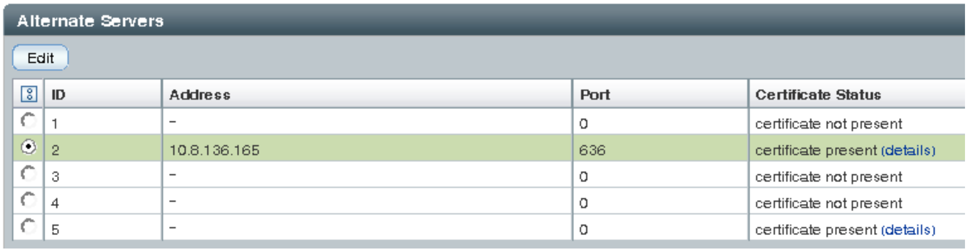
- **Alternate Servers table:**

  Use the Alternate Server table to view and configure properties for Microsoft Active Directory Alternate Servers.

  Alternate Servers configurations provide redundancy as well as a choice for when different servers are needed to isolate domains. If a certificate is not supplied, but is required, the top-level primary certificate is used. The alternate servers have the same rules and requirements as the top-level certificate mode. Each server has its own certificate status, and its own certificate command to retrieve the certificate if it is needed.

ID	Address	Port	Certificate Status
1	-	0	`certificate not present`
2	`10.8.136.165`	0	`certificate present (details)`

The following image shows an Alternate Servers table with a certificate present in ID 2:



Alternate Servers

Edit

	ID	Address	Port	Certificate Status
○	1	-	0	certificate not present
●	2	10.8.136.165	636	certificate present (details)
○	3	-	0	certificate not present
○	4	-	0	certificate not present
○	5	-	0	certificate present (details)

The following certificate information is displayed when you click on the “details” link:

Item	Description
Issuer	Certificate Authority who issued the certificate.
Subject	Server or domain for which the certificate is intended.
Valid From	Date when the certificate becomes valid.
Valid Until	Date when the certificate becomes invalid.
`Serial Number`	Serial number of the certificate.
Version	Version number of the certificate.

- **DNS Locator Queries Table:**

  Use the DNS Locator Queries table to view and configure Microsoft Active Directory DNS Locator Queries.

  The DNS Locator Queries table queries DNS servers to learn about the hosts to use for authentication.

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

  - _ldap._tcp.gc._msdcs.<DOMAIN>.<PORT:3269>
  - _ldap._tcp.dc._msdcs.<DOMAIN>.<PORT:636>

Note – DNS and DNS Locator Mode must be enabled for DNS Locator Queries to work.

---

6. **Click Save for your changes to take effect.**

▼ Troubleshoot Active Directory Authentication and Authorization (Web)

Before You Begin

- To configure Active Directory settings, you need the User Management (`u`) role enabled.
- To configure the Expanded Search Mode property, the server or CMM must be running Oracle ILOM firmware version 3.0.4 or later.
- To configure the Strict Credential Error Mode property, the server or CMM must be running Oracle ILOM firmware version 3.0.10 or later.

To troubleshoot the active directory authentication and authorization, follow these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface.**
2. **Click User Management --> Active Directory.**

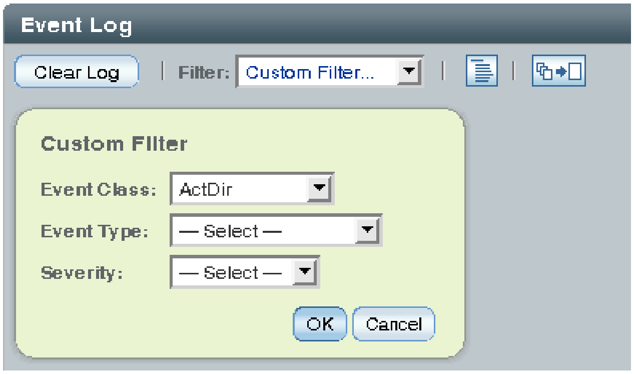
   The Active Directory page appears.
3. **In the Log Detail drop-down list, select the level of detail that you would like the event log to capture.**

   Choices are None, High, Medium, Low, and Trace.
4. **Click Save to save your changes.**

5. **Attempt an authentication to generate events. Follow these steps:**

   a. **From the System Monitoring tab select Event Logs.**

   b. **In the Filter drop-down list, select Custom Filter.**



Event Log

Clear Log | Filter: Custom Filter...

Custom Filter

Event Class: ActDir

Event Type: — Select —

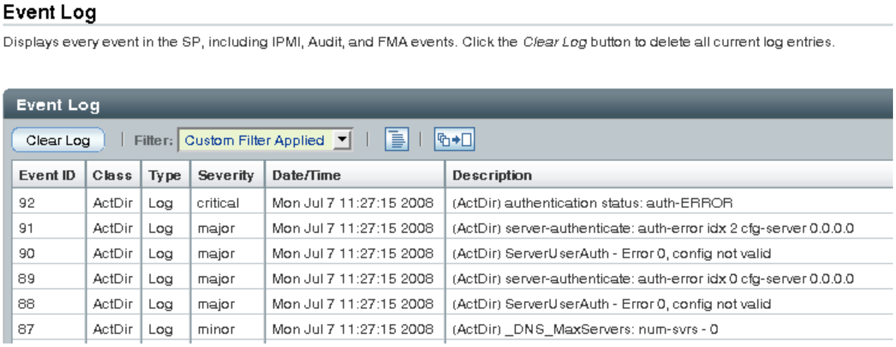
Severity: — Select —

OK Cancel

   c. **In the Event Class drop-down list, select ActDir.**

   d. **Click OK.**

   All Active Directory events will appear in the event log.



Event Log

Displays every event in the SP, including IPMI, Audit, and FMA events. Click the *Clear Log* button to delete all current log entries.

Event Log

Clear Log | Filter: Custom Filter Applied

Event ID	Class	Type	Severity	Date/Time	Description
92	ActDir	Log	critical	Mon Jul 7 11:27:15 2008	(ActDir) authentication status: auth-ERROR
91	ActDir	Log	major	Mon Jul 7 11:27:15 2008	(ActDir) server-authenticate: auth-error idx 2 cfg-server 0.0.0.0
90	ActDir	Log	major	Mon Jul 7 11:27:15 2008	(ActDir) ServerUserAuth - Error 0, config not valid
89	ActDir	Log	major	Mon Jul 7 11:27:15 2008	(ActDir) server-authenticate: auth-error idx 0 cfg-server 0.0.0.0
88	ActDir	Log	major	Mon Jul 7 11:27:15 2008	(ActDir) ServerUserAuth - Error 0, config not valid
87	ActDir	Log	minor	Mon Jul 7 11:27:15 2008	(ActDir) _DNS_MaxServers: num-svrs - 0

Configuring Lightweight Directory Access Protocol (LDAP)

Description	Links	Platform Feature Support
Manage LDAP settings in the Oracle ILOM web interface	• "Configure LDAP Server Settings (Web)" on page 63 • "Configure Oracle ILOM for LDAP (Web)" on page 64	• x86 system server SP • SPARC system server SP • CMM

▼ Configure LDAP Server Settings (Web)

Before You Begin

- To modify the LDAP Server settings in Oracle ILOM, you need the User Management (u) role enabled.

To configure the LDAP Server settings, follow these steps:

1. **Ensure that all user accounts authenticating to Oracle ILOM have user account passwords stored in a crypt format.**

   Oracle ILOM only supports LDAP authentication for passwords stored in one of the following two variations of crypt formats.

   ```
   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). See the following table for a description of the required property values.**

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

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

3. **Configure the LDAP server to enable LDAP server access to Oracle 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 Oracle ILOM.

   See your LDAP server documentation for more details.

▼ Configure Oracle ILOM for LDAP (Web)

Before You Begin

- To modify LDAP settings in Oracle ILOM, you need the User Management (u) role enabled.

To configure Oracle ILOM for LDAP, follows these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface.**

2. **Click User Management --> LDAP.**

   The LDAP Settings page appears.

3. **In the LDAP settings page, specify values for the following properties:**

   - **State** – Click the Enabled check box to authenticate LDAP users.
   - **Role** – In the Role drop-down list, specify a default LDAP user role (Administrator, Operator. or Advanced roles).
   - **Address** – In the Address text box, type the IP address or the DNS host name for the LDAP server.
   - **Port** – In the Port text box, accept the default LDAP port number (389) or modify the default port number.
   - **Searchbase** – In the Searchbase text box, type the branch of your LDAP server to search for users.
   - **Bind DN** – In the Bind DN text box. type the Distinguished Name (DN) of a read-only proxy user on the LDAP server. Oracle ILOM must have read-only access to your LDAP server to search and authenticate users.
   - **Bind Password** – In the Bind Password text box, type the password of the read-only user.

4. **Click Save for your changes to take effect.**

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

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

Configuring LDAP/SSL Settings (Web)

Description	Links	Platform Feature Support
Manage LDAP/SSL settings in the Oracle ILOM web interface	• "View and Configure LDAP/SSL Settings (Web)" on page 65 • "Configure LDAP/SSL Tables (Web)" on page 69 • "Troubleshoot LDAP/SSL Authentication and Authorization (Web)" on page 72	• x86 system server SP • SPARC system server SP • CMM

▼ View and Configure LDAP/SSL Settings (Web)

Before You Begin

- To modify LDAP/SSL settings in Oracle ILOM, you need the User Management (u) role enabled.
- To modify the Optional User Mapping property, the server must be running Oracle ILOM firmware version 3.0.4 or later.

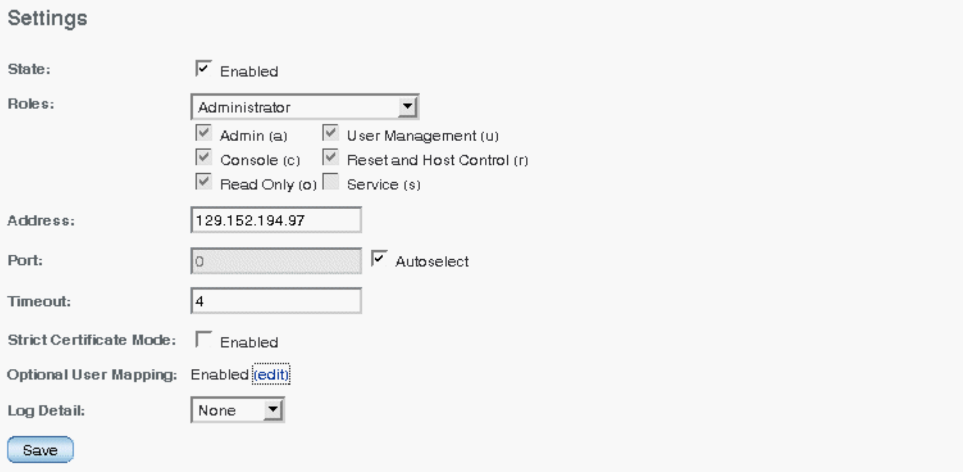
To view and configure LDAP/SSL settings, follow these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface.**

2. **Click User Management --> LDAP/SSL.**

   The LDAP/SSL page appears. There are three sections to the LDAP/SSL page.

   - The top section, which includes targets and properties:



Settings

State: ☑ Enabled

Roles: Administrator ▾

☑ Admin (a) ☑ User Management (u)
☑ Console (c) ☑ Reset and Host Control (r)
☑ Read Only (o) □ Service (s)

Address: 129.152.194.97

Port: 0 ☑ Autoselect

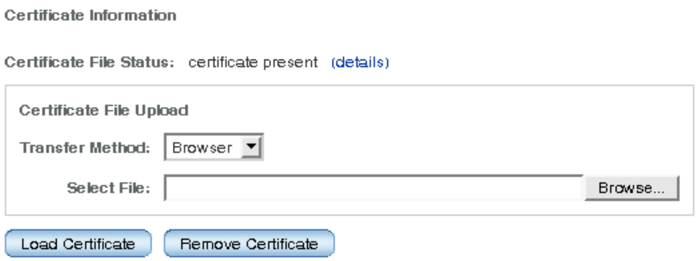
Timeout: 4

Strict Certificate Mode: □ Enabled

Optional User Mapping: Enabled (edit)

Log Detail: None ▾

- The middle section, which includes certificate information:



Certificate Information

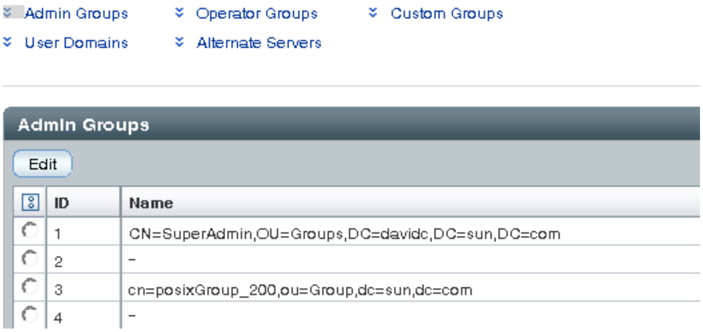
Certificate File Status: certificate present (details)

Certificate File Upload

Transfer Method: Browser ▾

Select File:

- The bottom section, which includes the LDAP/SSL tables:



Admin Groups

	ID	Name
○	1	CN=SuperAdmin,OU=Groups,DC=davidc,DC=sun,DC=com
○	2	-
○	3	cn=posixGroup_200,ou=Group,dc=sun,dc=com
○	4	-

3. **Configure the LDAP/SSL settings displayed in the top section of the LDAP/SSL Settings page.**

   See the following table for a description of the LDAP/SSL settings.

Property (Web)	Default	Description
State	Disabled	Enabled | Disabled
Roles	(none)	Administrator | Operator | Advanced | (none) Access role granted to all authenticated LDAP/SSL 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, o=Read-Only, and s=Service. If you do not configure a role, the LDAP/SSL server is used to determine the role.
Address	0.0.0.0	IP address or DNS name of the LDAP/SSL server.
Port	0	Port used to communicate with the server. If autoselect option is enabled, then the port is set to 0. Available in the unlikely event of a non-standard TCP port being used.
Timeout	4	Time-out value in seconds. Number of seconds to wait for individual transactions to complete. The value does not represent the total time of all transactions because the number of transactions can differ depending on the configuration. This property allows for tuning the time to wait when a server is not responding or is unreachable.
Strict Certificate Mode	Disabled	Enabled | Disabled If enabled, the server certificate contents are verified by digital signatures at the time of authentication. Certificate must be loaded before Strict Certificate Mode can be set to enabled.
Optional User Mapping	Disabled	Enabled | Disabled As of Oracle ILOM 3.0.4, optional user mapping is available. If enabled, alternative attributes other than the Distinguished Name (DN) can be used for user credential authentication. Use this property to convert a simple user login name to the DN for user credential validation. Click edit to enable and modify the User Attribute Mapping Parameters dialog, then click Save.
Log Detail	None	None | High | Medium | Low Specifies the amount of diagnostics that go into the event log.

4. **Click Save in the top section of the LDAP/SSL settings page to save any changes made to this section.**

5. **View the LDAP/SSL certificate information in the middle section of the LDAP/SSL settings page.**

   See the following table for a description of LDAP/SSL certificate settings.

Property	Displays	Description
Certificate File Status	Certificate not present	Read-only indicator of whether a certificate exists.
Certificate File Status	Certificatepres ent (details)	Click the (details) link to view certificate information about the issuer, subject, serial number, valid from, valid to, and version.

6. **If Strict Certificate Mode is enabled, perform the following steps:**

Note – When Strict Certificate Mode is disabled, the data will continue be protected but a certificate is not required.

---

   a. **Complete the "Certificate File Upload" section by specifying the following required parameters for uploading the certificate file**

Transfer Method	**Required Parameters**
Browser	File Name
TFTP	Host Filepath
FTP	Host Filepath Username Password
SCP	Host Filepath Username Password

   b. **To upload the certificate, click the Load Certificate button.**

   c. **When the certificate is loaded, click the (details) to view the following information about the certificate:**

Item	Description
Issuer	Certificate Authority who issued the certificate.
Subject	Server or domain for which the certificate is intended.
Valid From	Date when the certificate becomes valid.
Valid Until	Date when the certificate becomes invalid.
Serial Number	Serial number of the certificate.
Version	Version number of the certificate.

▼ Configure LDAP/SSL Tables (Web)

Before You Begin

- To modify LDAP/SSL settings in Oracle ILOM, you need the User Management (u) role enabled.
- To modify the Optional User Mapping property, the server must be running Oracle ILOM firmware version 3.0.4 or a later.

To configure LDAP/SSL tables, follow these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface.**
2. **Click User Management --> LDAP/SSL.**

   The LDAP/SSL page appears.
3. **At the bottom of the LDAP/SSL page, click the link to access the category of table you want to configure:**
   - Admin Groups
   - Operator Groups
   - Custom Groups
   - User Domains
   - Alternate Servers
4. **Enable the radio button of the individual table, and then click Edit.**
5. **Enter the required data in the tables.**

   In the following tables, default data shows the expected format of the LDAP/SSL data.
   - **Admin Groups table:**

The Admin Groups table contains the names of the LDAP/SSL groups in the Distinguished Name (DN) format.

ID	Name
1	CN=SpSuperAdmin,OU=Groups,DC=sales,DC=east,DC=oracle,DC=com
2	

- **Operator Groups table:**

  The Operator Groups table contains the names of the LDAP/SSL groups in the Distinguished Name (DN) format.

ID	Name
1	CN=SpSuperOper,OU=Groups,DC=sales,DC=east,DC=oracle,DC=com
2	

- **Custom Groups table**:

  The Custom Groups table contains the names of the LDAP/SSL groups in the Distinguished Name (DN) format, Simple Name format, or NT-Style Name. The associated roles for the entry are also configured. The name listed in entry 1 uses the Simple Name format.

ID	Name	Roles
1	custom_group_1	Admin, User Management, Console, Reset and Host Control, Read Only (aucro)

- **User Domains table:**

  User domains are the authentication domains used to authenticate a user. When the user logs in, the name used is formatted in the specific domain name format. User authentication is attempted based on the user name that is entered and the configured user domains.

  Entry 1 shows the complete Distinguished Name, which LDAP/SSL would use if the attempt to authenticate the first entry failed.

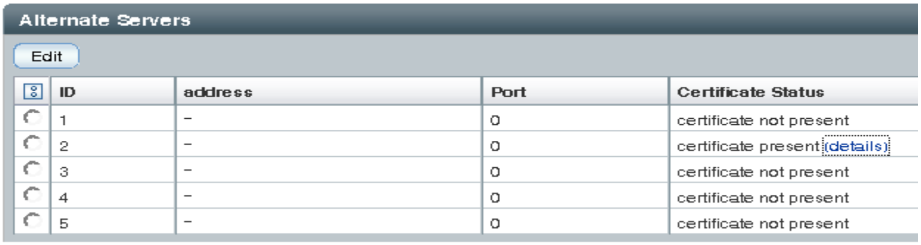
ID	Domain
1	`UID=<USERNAME>,OU=people,DC=oracle,DC=com`
2	

- **Alternate Servers table:**

  The Alternate Servers table provides redundancy for authentication. If a certificate is not supplied, but is required, the top-level primary certificate is used. The alternate servers have the same rules and requirements as the top-level certificate mode. Each server has its own certificate status, and its own certificate command to retrieve the certificate if it is needed.

ID	Address	Port	Certificate Status
1	-	0	`certificate not present`
2	-	0	`certificate not present`
3	`10.7.143.246`	0	`certificate present (details)`

The following image shows an Alternate Servers table with a certificate present in ID 2:



Alternate Servers

Edit

	ID	address	Port	Certificate Status
○	1	-	0	certificate not present
○	2	-	0	certificate present (details)
○	3	-	0	certificate not present
○	4	-	0	certificate not present
○	5	-	0	certificate not present

The following information is displayed when you click on the “details” link:

Item	Description
Issuer	Certificate Authority who issued the certificate.
Subject	Server or domain for which the certificate is intended.
Valid From	Date when the certificate becomes valid.

Valid Until	Date when the certificate becomes invalid.
Serial Number	Serial number of the certificate.
Version	Version number of the certificate.

▼ Troubleshoot LDAP/SSL Authentication and Authorization (Web)

Before You Begin

- To modify LDAP/SSL settings in Oracle ILOM, you need the User Management (u) role enabled.
- To modify the Optional User Mapping property, the server must be running Oracle ILOM firmware version 3.0.4 or a later.

To troubleshoot LDAP/SSL authentication, follow these steps:

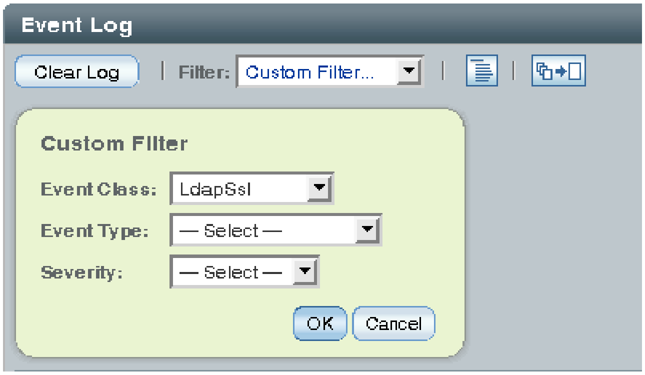
1. **Log in to the Oracle ILOM SP or CMM web interface.**
2. **Click User Management --> LDAP/SSL.**

   The LDAP/SSL page appears.
3. **In the Log Detail drop-down list, select the level of detail that you would like the event log to capture.**

   Choices are None, High, Medium, Low, and Trace.
4. **Click Save to save your changes.**
5. **Attempt an authentication to generate events, by performing these steps:**

   a. **Select System Monitoring --> Event Logs.**

   b. **In the Filter drop-down list, select Custom Filter.**



Filter: Custom Filter...

Event Class: LdapSsl

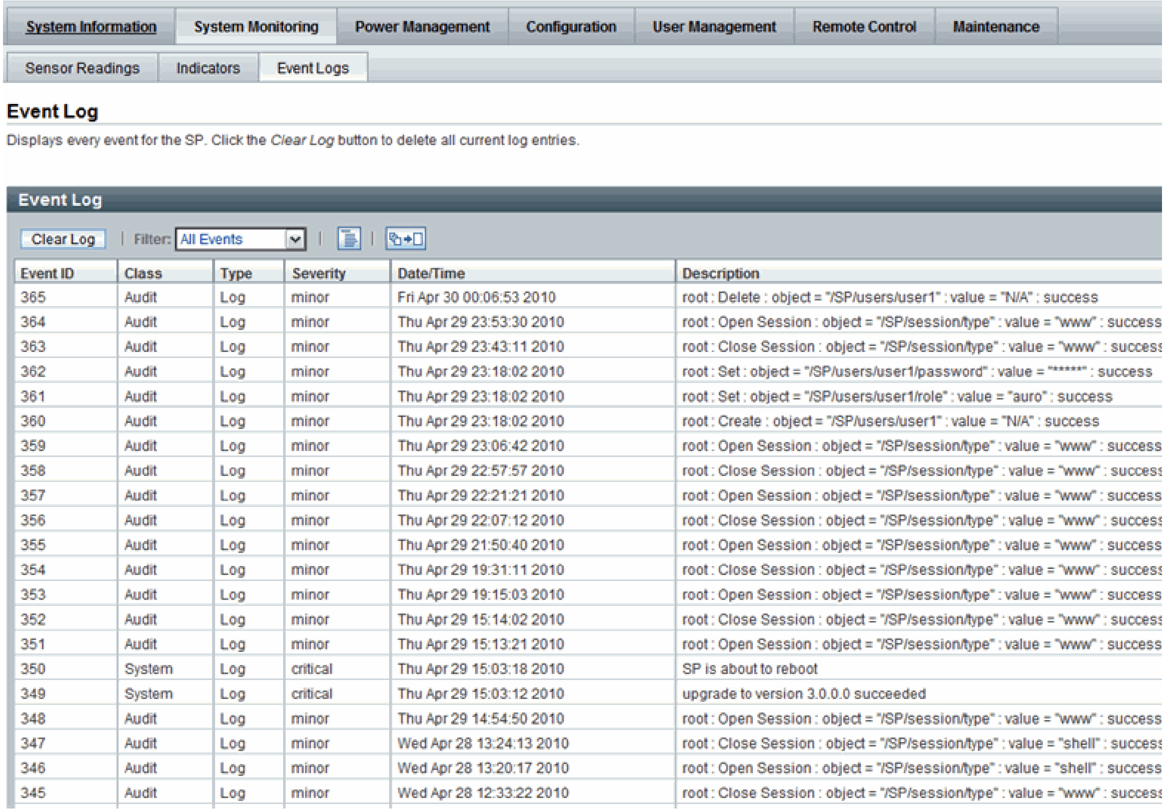
Event Type: — Select —

Severity: — Select —

c. **In the Event Class drop-down list, select LdapSsl.**

d. **Click OK for your changes to take effect.**

All LDAP/SSL events will appear in the event log.



Event Log

Displays every event for the SP. Click the *Clear Log* button to delete all current log entries.

Event Log

Event ID	Class	Type	Severity	Date/Time	Description
365	Audit	Log	minor	Fri Apr 30 00:06:53 2010	root : Delete : object = "/SP/users/user1" : value = "N/A" : success
364	Audit	Log	minor	Thu Apr 29 23:53:30 2010	root : Open Session : object = "/SP/session/type" : value = "www" : success
363	Audit	Log	minor	Thu Apr 29 23:43:11 2010	root : Close Session : object = "/SP/session/type" : value = "www" : success
362	Audit	Log	minor	Thu Apr 29 23:18:02 2010	root : Set : object = "/SP/users/user1/password" : value = "*****" : success
361	Audit	Log	minor	Thu Apr 29 23:18:02 2010	root : Set : object = "/SP/users/user1/role" : value = "auro" : success
360	Audit	Log	minor	Thu Apr 29 23:18:02 2010	root : Create : object = "/SP/users/user1" : value = "N/A" : success
359	Audit	Log	minor	Thu Apr 29 23:06:42 2010	root : Open Session : object = "/SP/session/type" : value = "www" : success
358	Audit	Log	minor	Thu Apr 29 22:57:57 2010	root : Close Session : object = "/SP/session/type" : value = "www" : success
357	Audit	Log	minor	Thu Apr 29 22:21:21 2010	root : Open Session : object = "/SP/session/type" : value = "www" : success
356	Audit	Log	minor	Thu Apr 29 22:07:12 2010	root : Close Session : object = "/SP/session/type" : value = "www" : success
355	Audit	Log	minor	Thu Apr 29 21:50:40 2010	root : Open Session : object = "/SP/session/type" : value = "www" : success
354	Audit	Log	minor	Thu Apr 29 19:31:11 2010	root : Close Session : object = "/SP/session/type" : value = "www" : success
353	Audit	Log	minor	Thu Apr 29 19:15:03 2010	root : Open Session : object = "/SP/session/type" : value = "www" : success
352	Audit	Log	minor	Thu Apr 29 15:14:02 2010	root : Close Session : object = "/SP/session/type" : value = "www" : success
351	Audit	Log	minor	Thu Apr 29 15:13:21 2010	root : Open Session : object = "/SP/session/type" : value = "www" : success
350	System	Log	critical	Thu Apr 29 15:03:18 2010	SP is about to reboot
349	System	Log	critical	Thu Apr 29 15:03:12 2010	upgrade to version 3.0.0.0 succeeded
348	Audit	Log	minor	Thu Apr 29 14:54:50 2010	root : Open Session : object = "/SP/session/type" : value = "www" : success
347	Audit	Log	minor	Wed Apr 28 13:24:13 2010	root : Close Session : object = "/SP/session/type" : value = "shell" : success
346	Audit	Log	minor	Wed Apr 28 13:20:17 2010	root : Open Session : object = "/SP/session/type" : value = "shell" : success
345	Audit	Log	minor	Wed Apr 28 12:33:22 2010	root : Close Session : object = "/SP/session/type" : value = "www" : success

Configuring RADIUS (Web)

Description	Links	Platform Feature Support
Manage RADIUS settings in the Oracle ILOM web interface	• "Configure RADIUS Settings (Web)" on page 74	• x86 system server SP • SPARC system server SP • CMM

▼ Configure RADIUS Settings (Web)

Before You Begin

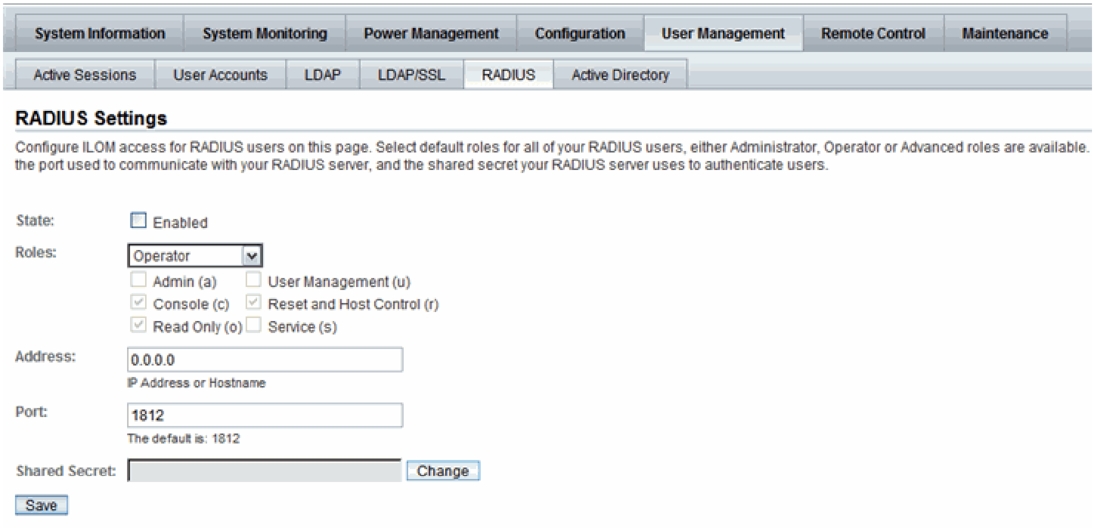
- To modify the RADIUS settings in Oracle ILOM, you must have the User Management (u) role enabled.

To modify the RADIUS settings, follow these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface.**

2. **Click User Management --> RADIUS.**

   The RADIUS Settings page appears.



RADIUS Settings

Configure ILOM access for RADIUS users on this page. Select default roles for all of your RADIUS users, either Administrator, Operator or Advanced roles are available. the port used to communicate with your RADIUS server, and the shared secret your RADIUS server uses to authenticate users.

State: □ Enabled

Roles: Operator

□ Admin (a) □ User Management (u)

☑ Console (c) ☑ Reset and Host Control (r)

☑ Read Only (o) □ Service (s)

Address: 0.0.0.0

IP Address or Hostname

Port: 1812

The default is: 1812

Shared Secret:

3. **In the RADIUS Settings page, specify values for the following web properties:**

Property (Web)	Default	Description
State	Disabled	Enabled | Disabled Specifies whether the RADIUS client is enabled or disabled.
Role	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, `o`=Read Only, and `s`= Service.
Address	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.
Shared Secret	(none)	Specifies the shared secret that is used to protect sensitive data and to ensure that the client and server recognize each other.

4. **Click Save for your changes to take effect.**

Managing Component Status and Service Actions (Web)

Description	Links
Web procedures for viewing and managing system component information and service actions.	• "View Component Status Information (Web)" on page 77 • "Prepare to Remove a Component (Web)" on page 79 • "Return a Component to Service (Web)" on page 79 • "Enable or Disable Components (Web)" on page 80 • "Clear Faults Detected by Oracle ILOM (Web)" on page 80

Related Information

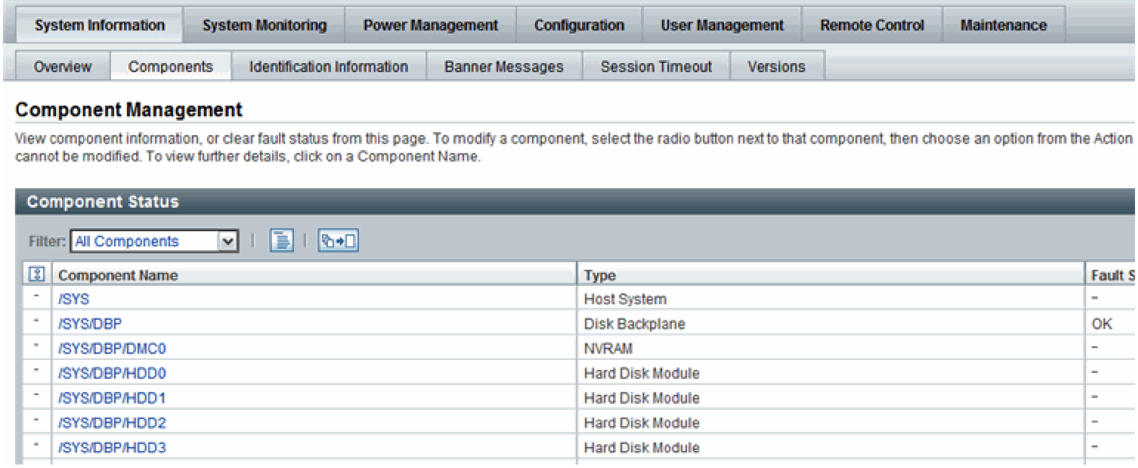
- *Oracle ILOM 3.0 Daily Management Concepts*, fault management
- *Oracle ILOM 3.0 Daily Management CLI Procedures*, manage component status and service actions

▼ View Component Status Information (Web)

To view component status information, follow these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface.**
2. **Click System Information --> Components.**

   The Component Management page appears.



Component Management

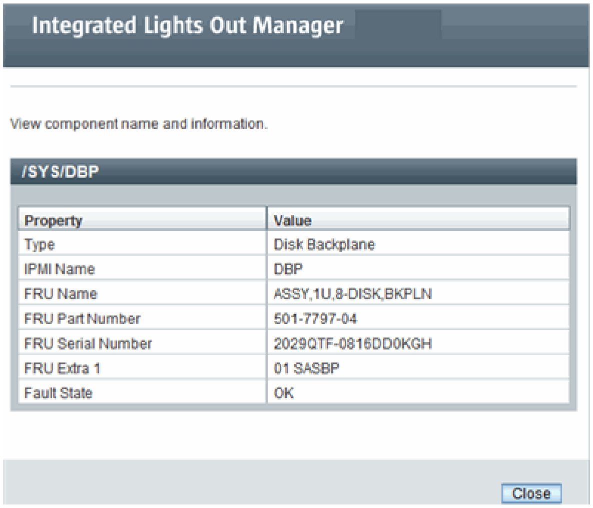
View component information, or clear fault status from this page. To modify a component, select the radio button next to that component, then choose an option from the Action cannot be modified. To view further details, click on a Component Name.

Component Status

	Component Name	Type	Fault S
-	/SYS	Host System	-
-	/SYS/DBP	Disk Backplane	OK
-	/SYS/DBP/DMC0	NVRAM	-
-	/SYS/DBP/HDD0	Hard Disk Module	-
-	/SYS/DBP/HDD1	Hard Disk Module	-
-	/SYS/DBP/HDD2	Hard Disk Module	-
-	/SYS/DBP/HDD3	Hard Disk Module	-

3. **When a component is faulted, a radio button will appear to the left of the component name. Click on the radio button to check the fault status. If a radio button does not appear next to a component's name, click on the name of a component to verify the status.**

   A dialog box appears with information about the selected component. See the following figure.



View component name and information.

/SYS/DBP

Property	Value
Type	Disk Backplane
IPMI Name	DBP
FRU Name	ASSY,1U,8-DISK,BKPLN
FRU Part Number	501-7797-04
FRU Serial Number	2029QTF-0816DD0KGH
FRU Extra 1	01 SASBP
Fault State	OK

▼ Prepare to Remove a Component (Web)

Before You Begin

- To manage system component operations in Oracle ILOM, the Reset and Host Control (r) role must be enabled.

To prepare the removal of a system component, follow these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface.**
2. **Select System Information --> Components.**

   The Component Management page appears.
3. **Select the radio button next to the component that you want to remove.**

   Components without radio buttons cannot be removed.
4. **From the Actions drop-down list, select Prepare to Remove.**

▼ Return a Component to Service (Web)

Before You Begin

- To manage system component operations in Oracle ILOM, the Reset and Host Control (r) role must be enabled.

Follow these steps to return a component to service:

1. **Log in to the Oracle ILOM SP or CMM web interface.**
2. **Select System Information --> Components.**

   The Component Management page appears.
3. **Select the radio button next to the component you want to return to service.**
4. **From the Actions drop-down list, select Return to Service.**

▼ Enable or Disable Components (Web)

Before You Begin

- To manage system component operations in Oracle ILOM, the Reset and Host Control (r) role must be enabled.

To enable or disable components, follow these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface.**
2. **Select System Information --> Components.**

   The Component Management page appears.
3. **Select the radio button next to the component you want to enable or disable.**
4. **From the Actions drop-down list, select either Enable or Disable.**

   The component is enabled or disabled, depending on your selection.

▼ Clear Faults Detected by Oracle ILOM (Web)

Before You Begin

- To clear faults in Oracle ILOM, you need the Admin (a) role enabled, and the server SP or CMM must be running Oracle ILOM firmware version 3.0.3 or later.

To view or clear faults using the Oracle ILOM web interface, follow these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface.**
2. **To view the status of faulted components detected by Oracle ILOM, do the following:**

   a. **Click System Information --> Fault Management.**

      The Fault Management page appears, listing faulted components by ID, FRU, and time-stamp.

   b. **To view additional information about the faulted component, click the faulted component ID.**

      Additional information about the faulted component appears in a dialog.

Note – Alternatively, you can view the fault status for a component in the Component Management page. In the Component Management page, select the component name to view the fault status information.

3. **Fix or replace the faulted component in the system.**

   After fixing or replacing the faulted component, you should clear the fault status in Oracle ILOM.

4. **To clear the status of faulted components shown in Oracle ILOM, do the following:**

   a. **Click the System Information --> Components tab.**

   b. **In the Component Management page, enable the radio button next to the faulted component, and then click Clear Faults.**

Monitoring System Sensors and Managing the Event Log (Web)

Description	Links
View sensor properties from Oracle ILOM	• "View Sensor Readings (Web)" on page 83
Manage system indicators, clock, and time-zone settings in Oracle ILOM	• "Configure System Indicators (Web)" on page 84 • "Configure Clock Settings (Web)" on page 85 • "Configure Time Zone Settings (Web)" on page 86
Filter, view, clear, and configure event logs from Oracle ILOM	• "Filter Event Log Output (Web)" on page 86 • "View and Clear Oracle ILOM Event Log (Web)" on page 88 • "Configure Remote Syslog Receiver IP Addresses (Web)" on page 89

Related Information

- *Oracle ILOM 3.0 Daily Management Concepts*, system monitoring and alert management
- *Oracle ILOM 3.0 Daily Management CLI Procedures*, monitor system sensors, indicators, and event logs
- *Oracle ILOM 3.0 Protocol Management Reference*, inventory and component management

▼ View Sensor Readings (Web)

To view sensor readings in Oracle ILOM, follow these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface.**

2. **Click System Monitoring --> Sensor Readings.**

   The Sensor Readings page appears.

Note – If the server is powered off, many components will appear as "no reading."

---

3. **In the Sensor Readings page, do the following:**

   a. **Locate the name of the sensor you want to configure.**

   b. **Click the name of the sensor to view the property values associated with that sensor.**

   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 (Web)

Before You Begin

- To configure the indicator state in Oracle ILOM, you need the User Management (`u`) role enabled.

To configure the system indicator states, follow these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface.**

2. **Click System Monitoring --> Indicators.**

   The Indicators page appears.

Note – If the server is powered off, many indicators will appear as "no reading."

---

3. **In the Indicators page, perform the following steps:**

   a. **Locate the name of the indicator you want to configure.**

   b. **To change the state of an indicator, click the radio button associated with the indicator that you want to change. Then in the Actions list box and select either Turn LED Off or Set LED to Fast Blink.**

   A dialog appears prompting you to confirm the change.

   c. **Click OK to confirm the change.**

▼ Configure Clock Settings (Web)

Before You Begin

- To set clock settings in Oracle ILOM, you need the Admin (a) role enabled.
- You need the IP address of your NTP server to complete this procedure.

To configure the clock settings, follow these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface.**
2. **Click Configuration --> Clock.**

   The Clock Settings page appears.
3. **In the Clock Settings page, do one of the following:**
   - View the existing settings.
   - Manually configure the date and time of the host server SP. See Step 4.
   - Synchronize the date and time of the host server SP with an NTP server. See Step 5.
4. **To manually set the date and time of the host server SP, follow these steps:**

   a. **In the Date text box, type the date in the format mm/dd/yy.**

   b. **In the Time list boxes, set the hour and minutes.**

   c. **Go to Step 6.**
5. **To configure an IP address of an NTP server and enable synchronization, follow these steps:**

   a. **Click the Enabled check box next to Synchronize Time Using NTP.**

   b. **In the Server 1 text box, type the IP address of the primary NTP server you want to use.**

   c. **(Optional) In the Server 2 text box, type the IP address of the secondary NTP server you want to use.**
6. **Click Save for your changes to take effect.**

   Refer to your Oracle Sun server platform user documentation for platform-specific clock information about whether:
   - The current time in Oracle ILOM persists across reboots of the SP.
   - The current time in Oracle ILOM can be synchronized with the host at host boot time.

- There is a real-time clock element that stores the time.

▼ Configure Time Zone Settings (Web)

Before You Begin

- To set clock time-zone settings in Oracle ILOM, you need the Admin (a) role enabled.

To configure a property value for the time-zone setting, follow these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface.**
2. **Click Configuration --> Timezone.**

   The Timezone Settings page appears.
3. **In the Timezone drop-down list, specify the appropriate time-zone setting.**

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

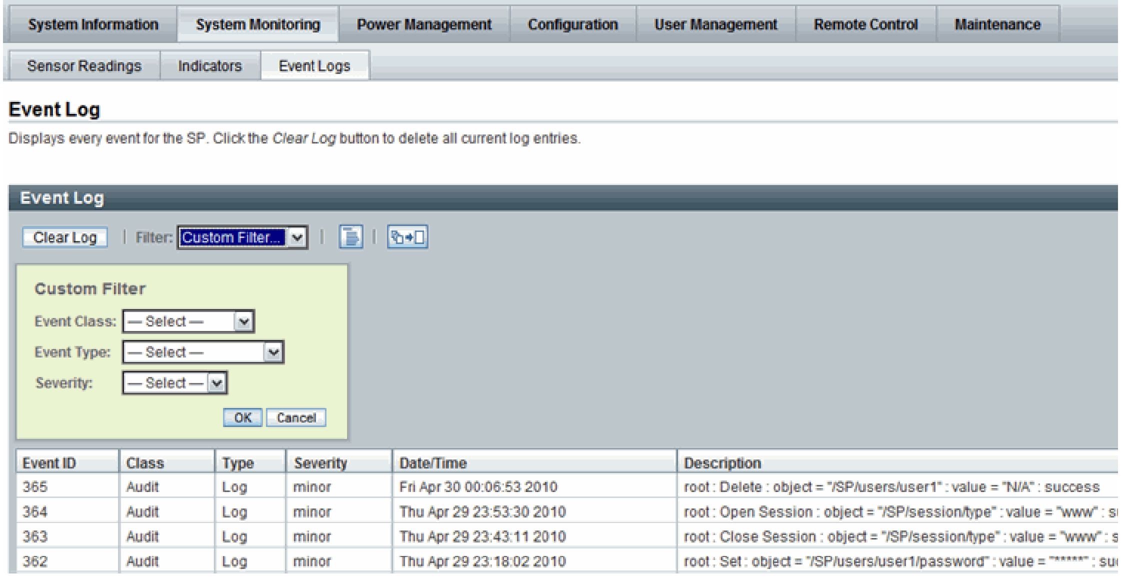
   - The current time in Oracle ILOM persists across reboots of the SP.
   - The current time in Oracle ILOM can be synchronized with the host at host boot time.
   - There is a real-time clock element that stores the time.

▼ Filter Event Log Output (Web)

To filter Oracle ILOM event log output, follow these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface.**
2. **Click System Monitoring --> Event Logs.**

   The Event Log page appears.



Event Log

Displays every event for the SP. Click the *Clear Log* button to delete all current log entries.

Event Log

Filter: Custom Filter...

Custom Filter

Event Class: — Select —

Event Type: — Select —

Severity: — Select —

Event ID	Class	Type	Severity	Date/Time	Description
365	Audit	Log	minor	Fri Apr 30 00:06:53 2010	root : Delete : object = "/SP/users/user1" : value = "N/A" : success
364	Audit	Log	minor	Thu Apr 29 23:53:30 2010	root : Open Session : object = "/SP/session/type" : value = "www" : s
363	Audit	Log	minor	Thu Apr 29 23:43:11 2010	root : Close Session : object = "/SP/session/type" : value = "www" : s
362	Audit	Log	minor	Thu Apr 29 23:18:02 2010	root : Set : object = "/SP/users/user1/password" : value = "*****" : su

3. **In the Filter list box on the Event Log page, click one of the following standard filters:**
   - All Events
   - Class: Fault
   - Type: Action
   - Severity: Down
   - Severity: Critical

4. **Alternatively, you can specify the following parameters for a Custom Filter.**

Event Class	Event Type	Severity
Developer	Log	Debug
Email	Connection	Down
Captive Shell	Send	Critical
Backup	Command Entered	Major
Restore	State	Minor
Reset	Action	
Chassis	Fault	
Audit	Repair	
IPMI	Warning	

Event Class	Event Type	Severity
Fault		
System		
ActDir		

View and Clear Oracle ILOM Event Log (Web)

Before You Begin

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

1. **Log in to the Oracle ILOM SP or CMM web interface.**
2. **Click System Monitoring --> Event Logs.**

   The Event Log page appears.
3. **In the Event Log page, perform any of the following:**
   - Page through entries – Use the page navigation controls at the top and the bottom of the table to navigate forward and back through the available data in the table.

     Note that selecting a greater number of entries might cause the web interface to respond slower than selecting a fewer number of entries.
   - View the entries in the display by scrolling through the list – 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 changes. • Chassis/Action – Category for shutdown events for server module/chassis, hot insert/removal of a FRU, and Reset Parameters button pressed. • Fault/Fault – For Fault Management faults. Description gives the time the fault was detected and suspect component. • Fault/Repair – For fault 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 Oracle ILOM time, the Oracle ILOM clock will use Universal Coordinated Time (UTC).
Description	A description of the event.

- Clear the event log – To clear the event log, click the Clear Event Log button. A confirmation dialog appears. In the confirmation dialog, click OK to clear the entries.

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

▼ Configure Remote Syslog Receiver IP Addresses (Web)

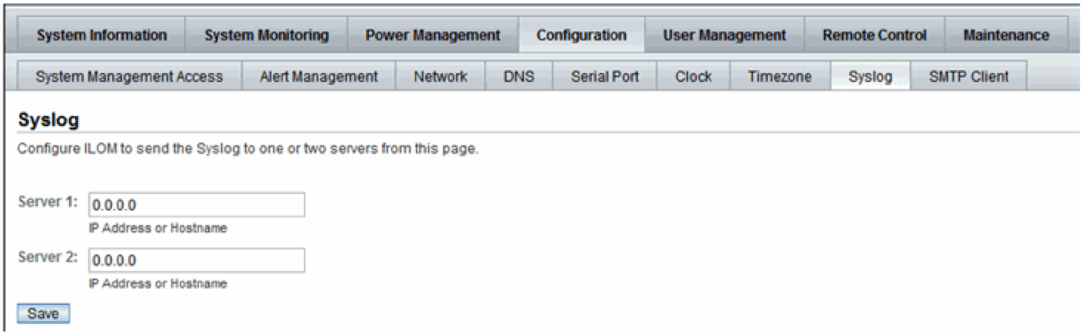
Before You Begin

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

To configure the remote syslog receiver IP addresses, follow these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface.**
2. **Click Configuration --> Syslog.**

   The Syslog page appears.



Syslog

Configure ILOM to send the Syslog to one or two servers from this page.

Server 1: 0.0.0.0
IP Address or Hostname

Server 2: 0.0.0.0
IP Address or Hostname

3. **In the IP Address 1 and 2 fields, type the IP addresses for the two locations to which you want to send syslog data.**
4. **Click Save for your settings to take effect.**

Monitoring Storage Components and Zone Manager (Web)

Description	Links
View and monitor storage details for HDDs and RAID controllers	• "Requirements for Monitoring Storage Components" on page 91 • "View and Monitor RAID Controller Details (Web)" on page 92 • "View and Monitor Details for Disks That Are Attached to RAID Controllers (Web)" on page 94 • "View and Monitor RAID Controller Volume Details (Web)" on page 95
Manage Zone Manager settings for SAS-2 storage devices that are installed in Sun Blade 6000 or 6048 series modular systems	• "Enabling or Disabling Zone Manager for SAS-2 Storage Devices" on page 96

Related Information

- *Oracle ILOM 3.0 Daily Management Concepts*, storage monitoring
- *Oracle ILOM 3.0 Daily Management CLI Procedures*, monitoring storage components
- *Oracle ILOM 3.0 CMM Administration*, zone manager

Requirements for Monitoring Storage Components

- Some Oracle servers might not support the storage monitoring functions that are described in this chapter. To determine whether the storage monitoring feature is enabled on your platform server, see the platform Oracle ILOM supplement guide or the platform server administration guide.

- For Oracle servers supporting the storage monitoring feature, you must download and install a hardware management pack prior to using the storage monitoring features in Oracle ILOM. For information about how to download this hardware management pack, see *Oracle Server Hardware Management Pack User's Guide*.
- The server must be running Oracle ILOM firmware version 3.0.8 or a later version.
- For conceptual information and examples on viewing and monitoring storage components, see the *Oracle ILOM 3.0 Daily Management Concepts Guide*.

▼ View and Monitor RAID Controller Details (Web)

Before You Begin

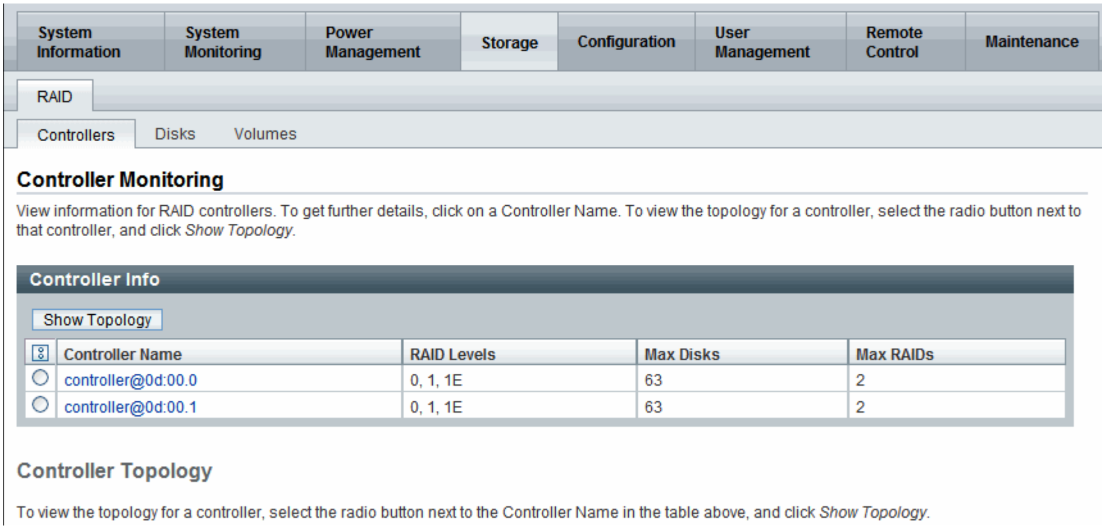
- Review the "Requirements for Monitoring Storage Components" on page 91.

To view and monitor RAID controller details, follow these steps:

1. **Log in to the Oracle ILOM SP web interface.**

2. **In the Oracle ILOM web interface, click Storage --> RAID --> Controllers.**

   The Controller Monitoring page appears listing the configuration details for the RAID controllers installed on your system.



Controller Monitoring

View information for RAID controllers. To get further details, click on a Controller Name. To view the topology for a controller, select the radio button next to that controller, and click *Show Topology*.

Controller Info

	Controller Name	RAID Levels	Max Disks	Max RAIDs
○	controller@0d:00.0	0, 1, 1E	63	2
○	controller@0d:00.1	0, 1, 1E	63	2

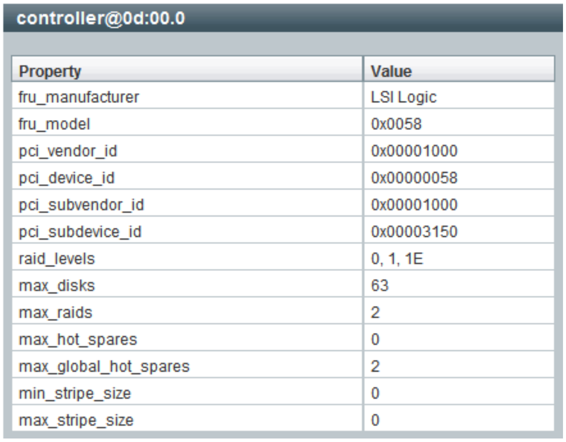
Controller Topology

To view the topology for a controller, select the radio button next to the Controller Name in the table above, and click *Show Topology*.

3. **To access additional details about an installed RAID controller, do the following:**

   - To access FRU properties and values, click the RAID controller name.

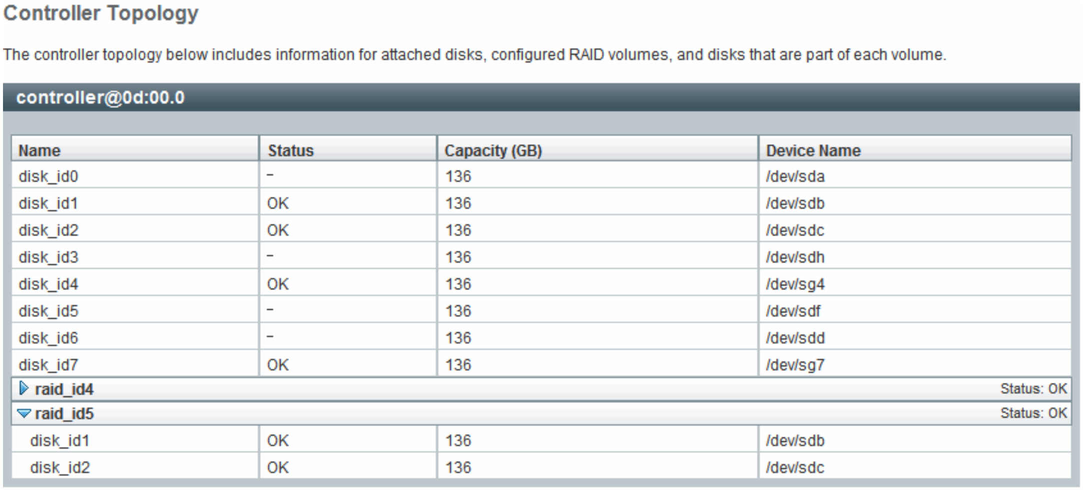
     A dialog appears listing the RAID controller FRU properties and values.



controller@0d:00.0

Property	Value
fru_manufacturer	LSI Logic
fru_model	0x0058
pci_vendor_id	0x00001000
pci_device_id	0x00000058
pci_subvendor_id	0x00001000
pci_subdevice_id	0x00003150
raid_levels	0, 1, 1E
max_disks	63
max_raids	2
max_hot_spares	0
max_global_hot_spares	2
min_stripe_size	0
max_stripe_size	0

   - To access topology information about a RAID controller, select the radio button next to the RAID controller name, then click Show Topology. The topology details for that RAID controller appear.



Controller Topology

The controller topology below includes information for attached disks, configured RAID volumes, and disks that are part of each volume.

controller@0d:00.0

Name	Status	Capacity (GB)	Device Name
disk_id0	-	136	/dev/sda
disk_id1	OK	136	/dev/sdb
disk_id2	OK	136	/dev/sdc
disk_id3	-	136	/dev/sdh
disk_id4	OK	136	/dev/sg4
disk_id5	-	136	/dev/sdf
disk_id6	-	136	/dev/sdd
disk_id7	OK	136	/dev/sg7
▷ **raid_id4**			Status: OK
▽ **raid_id5**			Status: OK
disk_id1	OK	136	/dev/sdb
disk_id2	OK	136	/dev/sdc

▼ View and Monitor Details for Disks That Are Attached to RAID Controllers (Web)

Before You Begin

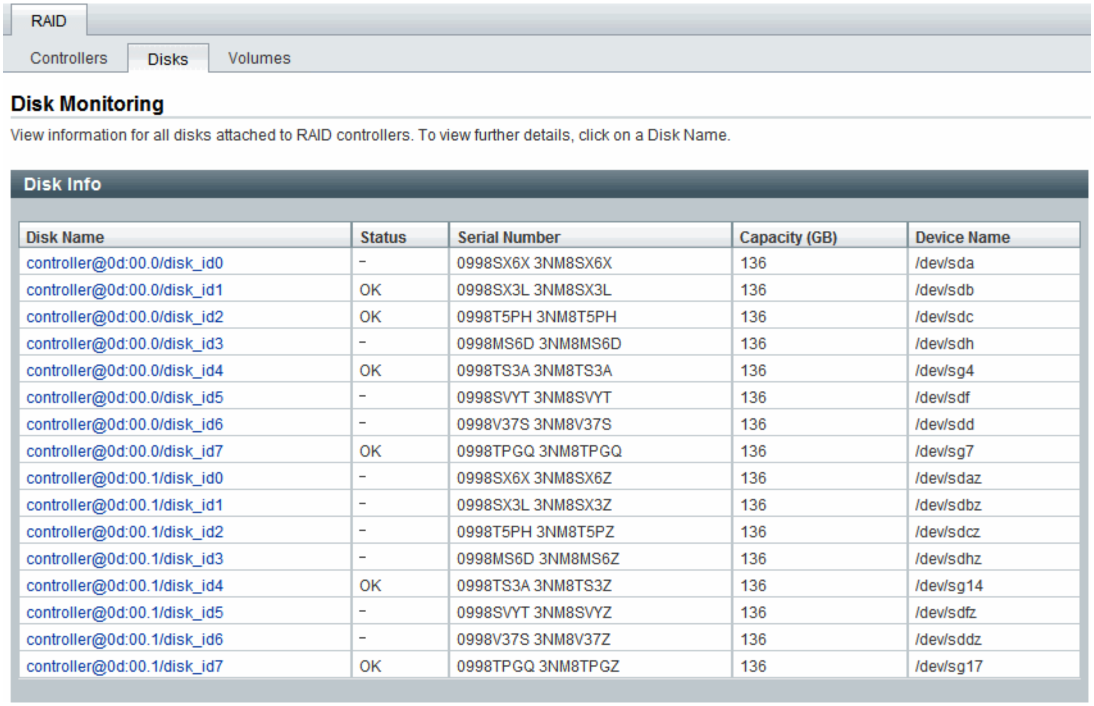
- Review the "Requirements for Monitoring Storage Components" on page 91.

To view and monitor details about storage disks attached to RAID controllers, follow these steps:

1. **Log in to the Oracle ILOM SP web interface.**

2. **In the Oracle ILOM web interface, click Storage --> RAID --> Disks.**

   The Disks Monitoring page appears listing the configuration details for the disks attached to RAID controllers.



Disk Monitoring

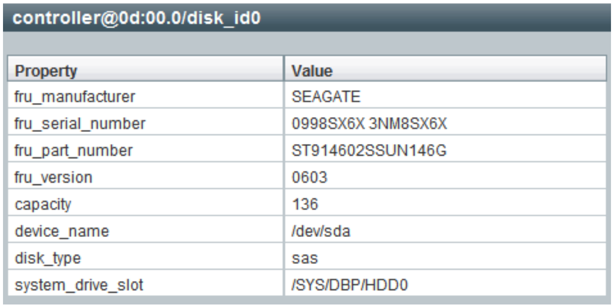
View information for all disks attached to RAID controllers. To view further details, click on a Disk Name.

Disk Info

Disk Name	Status	Serial Number	Capacity (GB)	Device Name
controller@0d:00.0/disk_id0	-	0998SX6X 3NM8SX6X	136	/dev/sda
controller@0d:00.0/disk_id1	OK	0998SX3L 3NM8SX3L	136	/dev/sdb
controller@0d:00.0/disk_id2	OK	0998T5PH 3NM8T5PH	136	/dev/sdc
controller@0d:00.0/disk_id3	-	0998MS6D 3NM8MS6D	136	/dev/sdh
controller@0d:00.0/disk_id4	OK	0998TS3A 3NM8TS3A	136	/dev/sg4
controller@0d:00.0/disk_id5	-	0998SVYT 3NM8SVYT	136	/dev/sdf
controller@0d:00.0/disk_id6	-	0998V37S 3NM8V37S	136	/dev/sdd
controller@0d:00.0/disk_id7	OK	0998TPGQ 3NM8TPGQ	136	/dev/sg7
controller@0d:00.1/disk_id0	-	0998SX6X 3NM8SX6Z	136	/dev/sdaz
controller@0d:00.1/disk_id1	-	0998SX3L 3NM8SX3Z	136	/dev/sdbz
controller@0d:00.1/disk_id2	-	0998T5PH 3NM8T5PZ	136	/dev/sdcz
controller@0d:00.1/disk_id3	-	0998MS6D 3NM8MS6Z	136	/dev/sdhz
controller@0d:00.1/disk_id4	OK	0998TS3A 3NM8TS3Z	136	/dev/sg14
controller@0d:00.1/disk_id5	-	0998SVYT 3NM8SVYZ	136	/dev/sdfz
controller@0d:00.1/disk_id6	-	0998V37S 3NM8V37Z	136	/dev/sddz
controller@0d:00.1/disk_id7	OK	0998TPGQ 3NM8TPGZ	136	/dev/sg17

3. **To view the FRU properties and values associated with a disk, click the disk name.**

   A dialog appears listing the disk FRU properties and values.



controller@0d:00.0/disk_id0

Property	Value
fru_manufacturer	SEAGATE
fru_serial_number	0998SX6X 3NM8SX6X
fru_part_number	ST914602SSUN146G
fru_version	0603
capacity	136
device_name	/dev/sda
disk_type	sas
system_drive_slot	/SYS/DBP/HDD0

▼ View and Monitor RAID Controller Volume Details (Web)

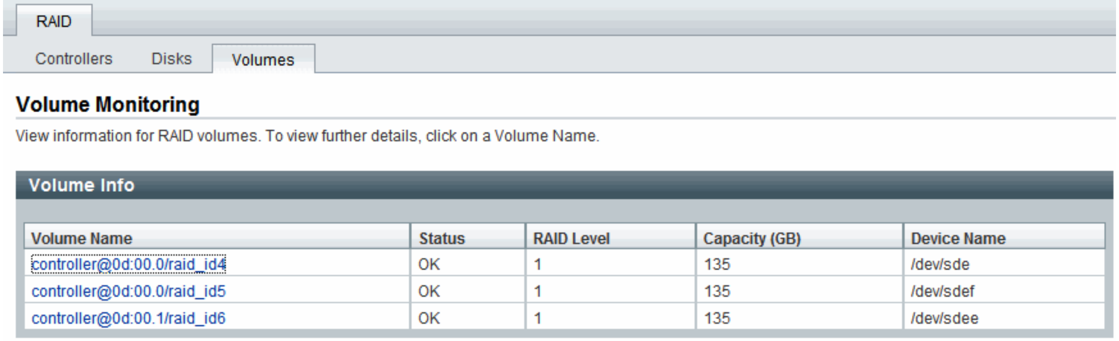
Before You Begin

- Review the "Requirements for Monitoring Storage Components" on page 91.

To view and monitor RAID controller volume details, follow these steps:

1. **Log in to the Oracle ILOM SP web interface.**
2. **In the Oracle ILOM web interface, click Storage --> RAID --> Volumes.**

   The Volume Monitoring page appears listing the configuration details for the RAID volumes configured on the RAID controllers.



Volume Monitoring

View information for RAID volumes. To view further details, click on a Volume Name.

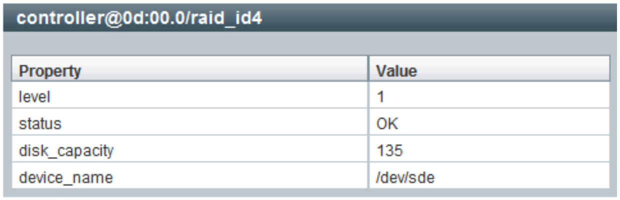
Volume Info

Volume Name	Status	RAID Level	Capacity (GB)	Device Name
controller@0d:00.0/raid_id4	OK	1	135	/dev/sde
controller@0d:00.0/raid_id5	OK	1	135	/dev/sdef
controller@0d:00.1/raid_id6	OK	1	135	/dev/sdee

3. **To view the FRU properties and values associated with a volume, click the volume name.**

   A dialog appears listing the volume properties and values.

View volume information.



controller@0d:00.0/raid_id4

Property	Value
level	1
status	OK
disk_capacity	135
device_name	/dev/sde

Enabling or Disabling Zone Manager for SAS-2 Storage Devices

If you are using Oracle Sun Blade 6000 or Sun Blade 6048 Modular Systems, a new zone management feature was added as of Oracle 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 Oracle ILOM, refer to the *Oracle ILOM 3.0 CMM Administration Guide for Sun Blade 6000 and Sun Blade 6048 Modular Systems*.

Managing System Alerts and Email Notifications (Web)

Description	Links
Identify requirements for managing system alerts	• "Managing Alert Rule Configurations (Web)" on page 98
Notify recipient of a system alerts using email	• "Configuring SMTP Client for Email Notification Alerts (Web)" on page 101

Related Information

- *Oracle ILOM 3.0 Daily Management Concepts*, system monitoring and alert management
- *Oracle ILOM 3.0 Daily Management CLI Procedures*, manage system alerts
- *Oracle ILOM 3.0 Protocol Management Reference*, inventory and component management

Managing Alert Rule Configurations (Web)

Description	Links	Platform Feature Support
Identify requirements for managing alerts	• "Requirements for Configuring Alert Rules" on page 98	• x86 system server SP • SPARC system server SP • CMM
Manage alert rule configurations	• "Create or Edit Alert Rules (Web)" on page 98 • "Disable an Alert Rule (Web)" on page 100 • "Send Test Alert for Specific Alert Rules (Web)" on page 100	

Requirements for Configuring Alert Rules

- If you are defining an Email Notification alert, the outgoing email server used to send the email notification must be configured in Oracle ILOM. If an outgoing email server is not configured, Oracle ILOM will not be able to successfully generate Email notifications.
- If you are defining an SNMP v3 trap alert, the SNMP user name must be defined in Oracle ILOM as an SNMP user. If the user is not defined as an SNMP user, the receiver of the SNMPv3 alert will not be able to decode the SNMP alert message.
- To manage alert rule configurations, you need the Admin (a) role enabled.
- To issue a test email alert from Oracle ILOM, the platform server or CMM must be running Oracle ILOM firmware version 3.0.4 or a later firmware version.

▼ Create or Edit Alert Rules (Web)

Before You Begin

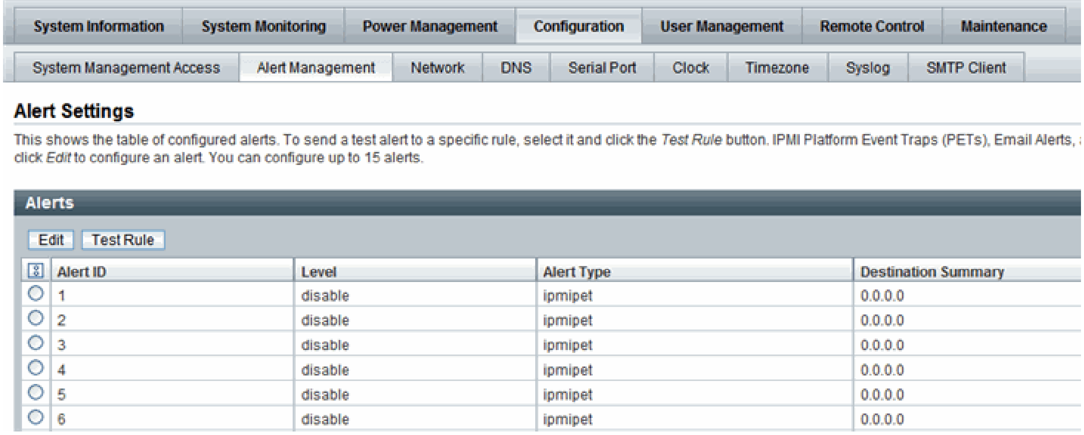
- Review the "Requirements for Configuring Alert Rules" on page 98.

T o configure alert rules in the Oracle ILOM web interface, follow these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface.**

2. **Click Configuration --> Alert Management.**

   The Alert Settings page appears.



Alert Settings

This shows the table of configured alerts. To send a test alert to a specific rule, select it and click the *Test Rule* button. IPMI Platform Event Traps (PETs), Email Alerts, : click *Edit* to configure an alert. You can configure up to 15 alerts.

Alerts

	Alert ID	Level	Alert Type	Destination Summary
○	1	disable	ipmipet	0.0.0.0
○	2	disable	ipmipet	0.0.0.0
○	3	disable	ipmipet	0.0.0.0
○	4	disable	ipmipet	0.0.0.0
○	5	disable	ipmipet	0.0.0.0
○	6	disable	ipmipet	0.0.0.0

3. **In the Alert Settings page, do the following:**

   a. **Enable the radio button for the alert rule you want to create or edit.**

   b. **In the Actions list box, select Edit.**

      A dialog appears displaying the property values associated with the alert rule.

   c. **In the properties dialog box, specify values for an alert type, alert level, and alert destination.**

      If the alert type you specify is for IPMI Pet, you need to define an IPMI Pet destination address.

      If the alert type you specify is for SNMP trap, you need to define an SNPMP destination address and port, as well as the SNMP version and community name.

      If the alert type you specify is for Email, you need to define a destination email address, and, if applicable, optional settings for filters and custom send options.

Note – You can specify one destination address for each alert rule type.

   For more information about the property values you can specify for an alert rule, refer to section about alert management in the *Oracle ILOM 3.0 Daily Management Concepts Guide*.

   d. **Click Save to apply the values specified and to close the properties dialog.**

▼ Disable an Alert Rule (Web)

Before You Begin

- Review the "Requirements for Configuring Alert Rules" on page 98.

To disable an alert rule in the Oracle ILOM web interface, follow these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface.**
2. **Click Configuration --> Alert Management.**

   The Alert Settings page appears.
3. **In the Alert Settings page, enable the radio button for the alert rule you want to disable, and then in the Actions list box, click Edit.**

   A dialog appears presenting properties you can define about the alert rule.
4. **In the properties dialog box, click Disabled in the Alert Levels list box.**
5. **Click Save to apply your changes and to close the properties dialog.**

▼ Send Test Alert for Specific Alert Rules (Web)

Before You Begin

- Review the "Requirements for Configuring Alert Rules" on page 98.

To send a test email alert for one or more alert rules, follow these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface.**
2. **Click Configuration --> Alert Management.**
3. **In the Alert Settings page, perform the following steps to send a test email alert:**

   a. **Enable the radio button next to each alert rule that you want to test.**

   b. **Click the Test Rule button to send a text email alert to the alert rule destination.**

Note – For each alert rule, one of the following alert types can be configured: IPMI PET destination address, Email destination address, and SNMP trap destination address. To configure the alert type, refer to "Create or Edit Alert Rules (Web)" on page 98.

Configuring SMTP Client for Email Notification Alerts (Web)

Description	Links	Platform Feature Support
Notify recipient of system alerts using email	• "Enable SMTP Client for Email Alerts (Web)" on page 101	• x86 system server SP • SPARC system server SP • CMM

▼ Enable SMTP Client for Email Alerts (Web)

Before You Begin

- To enable SMTP clients, you need the Admin (a) role enabled.
- To generate configured email notification alerts, you must enable the Oracle ILOM client to act as an SMTP client to send the email alert messages.
- Prior to enabling the Oracle 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.

1. **Log in to the Oracle ILOM SP or CMM web interface.**
2. **Click Configuration --> SMTP Client.**

   The SMTP Client page appears.
3. **In the SMTP Client page, specify the following settings to enable the sending of Email Notification alerts.**

SMTP Setting	Description
SMTP State	Enable the SMTP State check box.
SMTP Server IP	Type the IP address of the outgoing SMTP email server that will process the email notifications.
SMTP Port	Type the port number of the outgoing SMTP email server.

4. **Click Save to apply the SMTP settings.**

Power Monitoring and Management of Hardware Interfaces (Web)

Description	Links
Identify power monitoring and management feature updates per Oracle ILOM firmware point release	• "Summary of Power Management Feature Updates (Web)" on page 104
Perform power monitoring and management of hardware interfaces from Oracle ILOM	• "Monitoring System Power Consumption (Web)" on page 106 • "Configuring Power Policy Settings to Manage Server Power Usage (Web)" on page 110 • "Configuring Power Consumption Threshold Notifications (Web)" on page 114 • "Monitoring and Configuring Component Power Allocation Distributions (Web)" on page 115 • "Configuring Server Power Limit Properties (Web)" on page 126 • "Monitoring or Configuring CMM Power Supply Redundancy (Web)" on page 129

Related Information

- *Oracle ILOM 3.0 Daily Management Concepts*, power consumption
- *Oracle ILOM 3.0 Daily Management CLI Procedures*, monitor and manage power consumption
- *Oracle ILOM 3.0 Protocol Management Reference*, monitor and manage power consumption

Summary of Power Management Feature Updates (Web)

The following table identifies power management feature enhancements and documentation updates made since Oracle ILOM 3.0.

TABLE: Power Management Feature Updates

New or Enhanced Feature	Firmware Point Release	Documentation Updates	For Updated Web Procedures, See:
Monitor power consumption metrics	Oracle 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 (Web)" on page 106
Configure power policy properties	Oracle 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 (Web)" on page 110
Monitor power consumption history	Oracle ILOM 3.0.3	• New power consumption history metrics • New CLI and web procedures added for monitoring power consumption	• "Monitor Power History Statistics (Web)" on page 108
Configure power consumption notification thresholds	Oracle 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 (Web)" on page 114
Monitor allocation power distribution metrics	Oracle 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 and Configuring Component Power Allocation Distributions (Web)" on page 115
Configure power budget properties	Oracle ILOM 3.0.6	• New power budget properties • New CLI and web procedures added for configuring power budget properties	• "Configuring Server Power Limit Properties (Web)" on page 126

TABLE: Power Management Feature Updates *(Continued)*

New or Enhanced Feature	Firmware Point Release	Documentation Updates	For Updated Web Procedures, See:
Configure power supply redundancy properties for CMM systems	Oracle ILOM 3.0.6	• New power supply redundancy properties for CMM systems • New CLI and web procedures added for configuring power supply redundancy properties on CMM systems	• "Monitoring or Configuring CMM Power Supply Redundancy (Web)" on page 129
Server power Allocation tab replaces Distribution tab	Oracle ILOM 3.0.8	• Oracle ILOM web Allocation tab replaces Distribution tab for server SPs • New web procedure added for viewing server power allocation properties	• "Monitoring and Configuring Component Power Allocation Distributions (Web)" on page 115
Server Limit tab Replaces Budget tab	Oracle ILOM 3.0.8	• Oracle ILOM web Limit tab replaces Budget tab for server SPs • New web procedure added for configuring power limit properties	• "Configuring Server Power Limit Properties (Web)" on page 126
Web interface layout update for CMM power management	Oracle ILOM 3.0.10	• New top-level tab added to Oracle ILOM web interface for power management • Revised Oracle ILOM web Power Consumption tab properties for CMMs • Oracle ILOM web Allocation tab replaces Distribution tab for CMMs • Power Management Metrics tab removed from CMM Oracle ILOM web interface • Updated web procedure for configuring a grant limit for blade slots (previously known as allocatable power)	• "Monitor System Power Consumption (Web)" on page 107 • "View CMM Component Power Allocations" on page 120 • "Configure Grant Limit for Blade Slots in CMM as of Oracle ILOM 3.0.10" on page 124 • "View CMM Component Power Allocations" on page 120
Power Management Statistic tab	Oracle ILOM 3.0.14	• The Power Statistics table on the History tab was moved to a Power Management --> Statistics tab	• "Monitor Power History Statistics (Web)" on page 108

Monitoring System Power Consumption (Web)

Description	Links	Platform Feature Support
Review the prerequisites for monitoring system power consumption.	• "Requirements for Monitoring Power Consumption (Web)" on page 106	• x86 server SP • SPARC server • CMM
Monitor power consumption properties from Oracle ILOM.	• "Monitor System Power Consumption (Web)" on page 107 • "Monitor Individual Power Supply Consumption (Web)" on page 108	
Monitor power consumption history from Oracle ILOM	• "Monitor Power History Statistics (Web)" on page 108	

Requirements for Monitoring Power Consumption (Web)

Prior to performing the procedures described in this section, you should ensure that the following requirements are met:

- Review the power monitoring terminology defined in the *Oracle ILOM 3.0 Daily Management Concepts Guide.*
- Review the web interface enhancements described in the section about system power consumption metrics in the *Oracle ILOM 3.0 Daily Management Concepts Guide.*

Note – The power consumption features described in this section might not be implemented on the platform server or CMM that you are using. To determine whether the power consumption features described in this section are supported on your server or CMM, see the Oracle ILOM supplement or administration guide provided for your server or CMM.

- To access the power consumption metrics provided in Oracle ILOM the server must be running Oracle ILOM firmware version 3.0 or later. To access the power consumption history metrics provided in Oracle ILOM, the server must be running Oracle ILOM firmware version 3.0.3 or later. To access the enhanced power consumption properties and the threshold notification properties provided in Oracle ILOM, the server must be running Oracle ILOM firmware version 3.0.4 or later.

Note – Power consumption history is provided using the Oracle ILOM CLI and web interfaces. This information is not available through IPMI or SNMP.

▼ Monitor System Power Consumption (Web)

Before You Begin

- Review the "Requirements for Monitoring Power Consumption (Web)" on page 106.

To monitor the total system power consumption, follow these steps:

1. **Log in to the Oracle ILOM SP or CMM web interface.**
2. **In the Oracle ILOM web interface, do one of the following:**
   - If the server or CMM is running Oracle ILOM firmware version 3.0.3 or later, click Power Management -->Consumption.
   - If the server or CMM is running an earlier firmware version that is prior to Oracle ILOM 3.0.3, click System Monitoring --> Power Management.

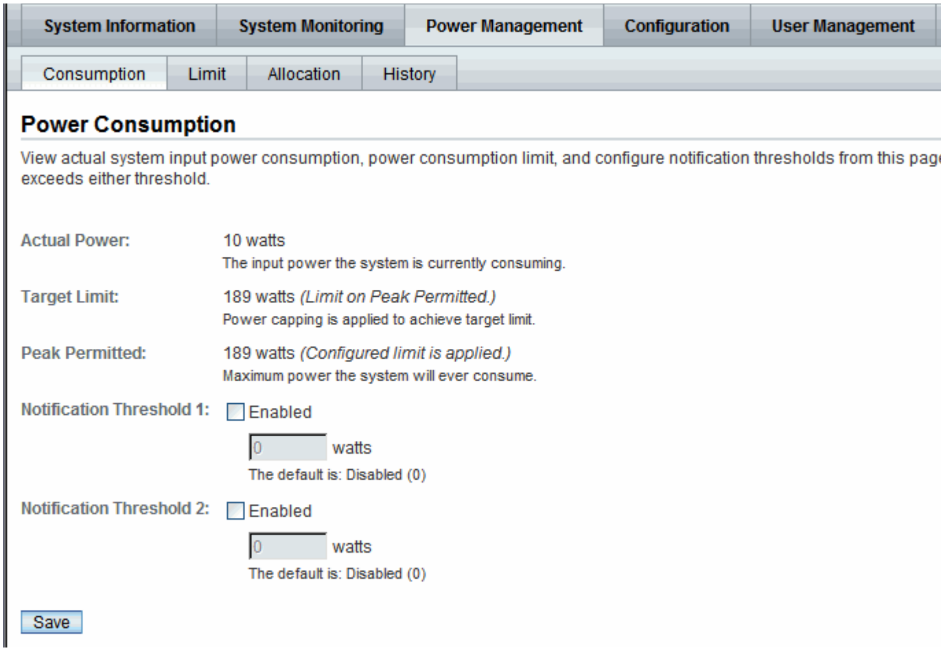
   The Power Consumption page appears.

Note – The ability to monitor power varies depending on the platform server implementation for this feature. Refer to the Oracle ILOM supplement or platform administration guide for platform-specific details or procedures about this feature.

---

3. **In the Power Consumption page, you can view power metrics provided for actual power, target limit, and peak permitted.**

Note – The properties on the Power Consumption page were updated for server SPs as of Oracle ILOM firmware version 3.0.8, and for CMMs as of Oracle ILOM firmware version 3.0.10. For more information about these properties, refer to the section about web enhancements for power metrics in the *Oracle ILOM 3.0 Daily Management Concepts Guide.*



Power Consumption

View actual system input power consumption, power consumption limit, and configure notification thresholds from this pag exceeds either threshold.

Actual Power: 10 watts
The input power the system is currently consuming.

Target Limit: 189 watts *(Limit on Peak Permitted.)*
Power capping is applied to achieve target limit.

Peak Permitted: 189 watts *(Configured limit is applied.)*
Maximum power the system will ever consume.

Notification Threshold 1: □ Enabled
0 watts
The default is: Disabled (0)

Notification Threshold 2: □ Enabled
0 watts
The default is: Disabled (0)

▼ Monitor Individual Power Supply Consumption (Web)

- **See the instructions for viewing sensors in**"View Sensor Readings (Web)" on page 83**.**

▼ Monitor Power History Statistics (Web)

Before You Begin

- Review the "Requirements for Monitoring Power Consumption (Web)" on page 106.

To monitor the power history statistics, follow these steps:

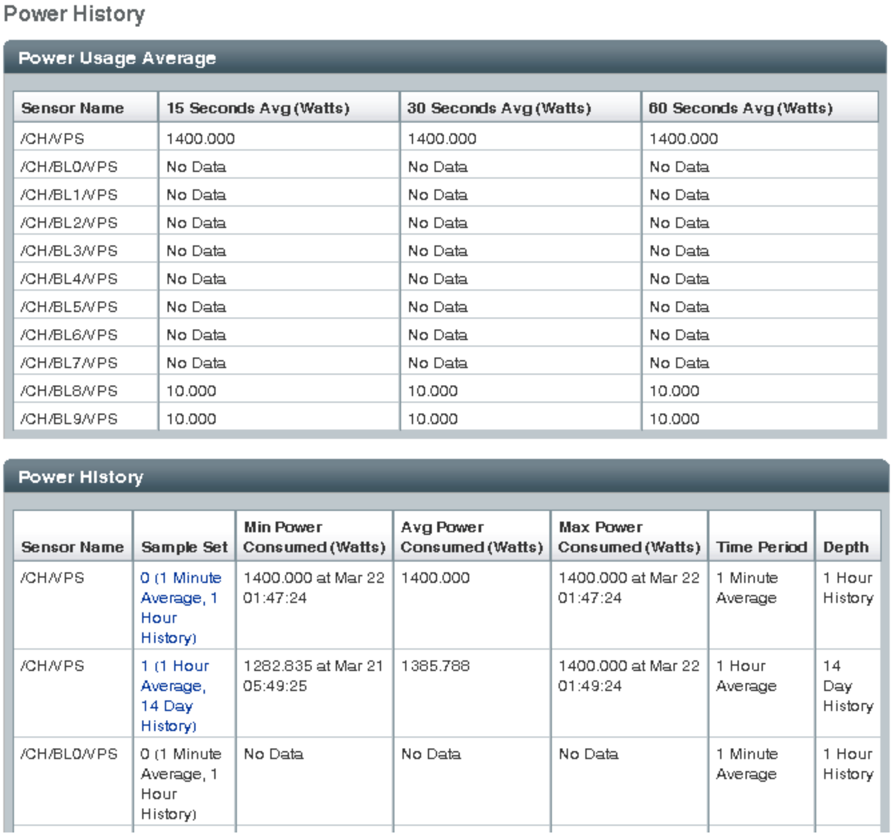
1. **Log in to Oracle ILOM SP or CMM web interface.**
2. **In the Oracle ILOM web interface, do one of the following:**
   - If the server or CMM is running Oracle ILOM firmware prior to Oracle ILOM 3.0.3, click System Monitoring --> Power Management, and then click the Power History link.

- If the server or CMM is running Oracle ILOM firmware version 3.0.3 or later, click Power Management --> History.
- If the server or CMM is running Oracle ILOM firmware version 3.0.14 or later, click Power Management --> Statistics to view the power statistics, or click Power Management --> History to view the power history.

Refer to the section about power monitoring terminology in the *Oracle ILOM 3.0 Daily Management Concepts Guide* for definitions describing the power monitoring history terms.

Note – The Statistic table available on the History tab as of Oracle ILOM firmware version 3.0.3 was moved to the Statistic tab in Oracle ILOM firmware version 3.0.14.

CMM Power History Example



Power History

Power Usage Average

Sensor Name	15 Seconds Avg (Watts)	30 Seconds Avg (Watts)	60 Seconds Avg (Watts)
/CH/VPS	1400.000	1400.000	1400.000
/CH/BL0/VPS	No Data	No Data	No Data
/CH/BL1/VPS	No Data	No Data	No Data
/CH/BL2/VPS	No Data	No Data	No Data
/CH/BL3/VPS	No Data	No Data	No Data
/CH/BL4/VPS	No Data	No Data	No Data
/CH/BL5/VPS	No Data	No Data	No Data
/CH/BL6/VPS	No Data	No Data	No Data
/CH/BL7/VPS	No Data	No Data	No Data
/CH/BL8/VPS	10.000	10.000	10.000
/CH/BL9/VPS	10.000	10.000	10.000

Power History

Sensor Name	Sample Set	Min Power Consumed (Watts)	Avg Power Consumed (Watts)	Max Power Consumed (Watts)	Time Period	Depth
/CH/VPS	0 (1 Minute Average, 1 Hour History)	1400.000 at Mar 22 01:47:24	1400.000	1400.000 at Mar 22 01:47:24	1 Minute Average	1 Hour History
/CH/VPS	1 (1 Hour Average, 14 Day History)	1282.835 at Mar 21 05:49:25	1385.788	1400.000 at Mar 22 01:49:24	1 Hour Average	14 Day History
/CH/BL0/VPS	0 (1 Minute Average, 1 Hour History)	No Data	No Data	No Data	1 Minute Average	1 Hour History

3. **To view a sample data set of power consumed by a device for a specific duration, click the link appearing under the Sample Set column in the Power History table.**

Configuring Power Policy Settings to Manage Server Power Usage (Web)

Description	Links	Platform Feature Support
Review the prerequisites for configuring the power policy and usage properties	• "Requirements for Configuring the Power Policy (Web)" on page 110	• x86 server SP • SPARC servers
Configure policy to control power consumption	• "Configure Power Consumption Policy (Web)" on page 111	• x86 server SP (prior to Oracle ILOM 3.0.4) • SPARC servers
Configure policy to control power capping	• "Configure Server Power Policy For Power Capping (Web)" on page 112	• x86 server SP • SPARC servers

Requirements for Configuring the Power Policy (Web)

Prior to performing the procedures described in this section, you should ensure that the following requirements are met:

- Review the power monitoring terminology defined in the *Oracle ILOM 3.0 Daily Management Concepts Guide.*
- Review the web interface enhancements described in the section about power policy settings in the *Oracle ILOM 3.0 Daily Management Concepts Guide.*

Note – The power policy features described in this section might not be implemented on the platform server that you are using. To determine whether the power policy features described in this section are supported on your server, refer to the Oracle ILOM supplement or administration guide provided for your server.

- To configure the power consumption policy properties in Oracle ILOM for x86 servers, you must have Admin (a) role privileges enabled, and the server must be running Oracle ILOM firmware version 3.0.3 or earlier.

- To configure the power consumption policy properties in Oracle ILOM for SPARC servers, you must have Admin (a) role privileges enabled, and the server must be running Oracle ILOM firmware version 3.0 or later.
- To configure the policy for powering capping on the Limit tab of the web interface, you must have Admin (a) role privileges enabled, and the server must be running Oracle ILOM firmware version 3.0.8 or later.

▼ Configure Power Consumption Policy (Web)

Before You Begin

- Review the "Requirements for Configuring the Power Policy (Web)" on page 110.

To configure the power consumption policy for an Oracle Sun server, follow these steps:

1. **Log in to the Oracle ILOM SP web interface.**

2. **In the Oracle ILOM web interface, do one of the following:**

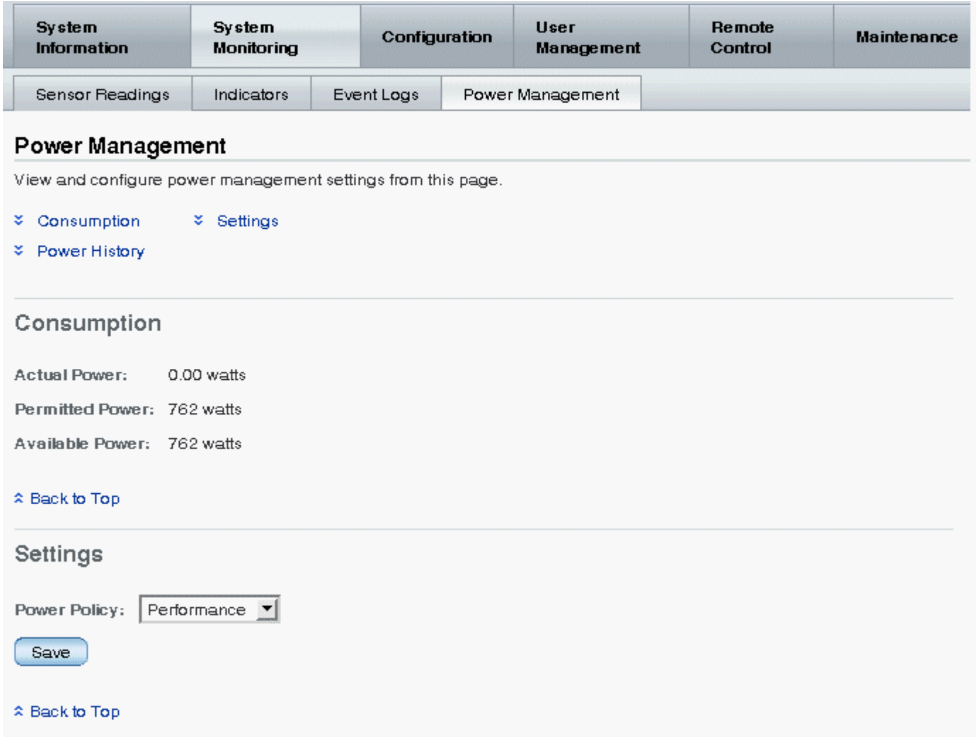
   - If the server is running firmware earlier than Oracle ILOM 3.0.3, click System Monitoring --> Power Management to view the Power Policy settings.

Note – The Power Policy settings on the Power Management Consumption page were removed from the Oracle ILOM web interface for x86 servers as of Oracle ILOM 3.0.4.

   - If the server is running Oracle ILOM firmware version 3.0.4 or later on a SPARC server, click Power Management --> Settings to view the Power Policy settings.

3. **In the Power Policy list box, click either Performance or Elastic.**

   - **Performance** – The system is allowed to use all of the power that is available.
   - **Elastic** – The system power usage is adapted to the current utilization level. For example, the system will power up or down just enough system components to keep relative utilization at 70 percent at all times, even if workload fluctuates.



Power Management

View and configure power management settings from this page.

Consumption

Actual Power: 0.00 watts

Permitted Power: 762 watts

Available Power: 762 watts

Settings

Power Policy: Performance

Note – The Power Policy settings were removed in Oracle ILOM 3.0.4 from the web and CLI interface for x86 servers.

---

4. **To apply the new setting, click Save.**

▼ Configure Server Power Policy For Power Capping (Web)

Before You Begin

- Review the "Requirements for Configuring the Power Policy (Web)" on page 110.

To configure the server power limit for power capping, follow these steps:

1. **Log in to the Oracle ILOM SP web interface.**

2. **In the Oracle ILOM web interface, click Power Management --> Limit.**

3. **In the Power Limit page, configure the policy settings for power capping as described in the following table.**

Property	Description
Policy	The Policy property enables you to configure the power capping policy. In the Policy property, specify which of the following types of power capping you want to apply: • **Soft - Only cap if actual power exceeds target limit.** If you enabled the soft cap option, you can configure the grace period for capping actual power to within the target limit. - **System default**. This option, when selected, applies the default optimum grace period property values that is specified by the platform server. *or* - **Custom**. This option, when selected, applies the grace period property value specified by the user. • **Hard - Fixed cap keeps peak permitted power under target limit**. If you enable this hard cap option, power capping is permanently set on the server without a grace period.
Violation Actions	The Violation Actions property enables you to specify the settings you want Oracle ILOM to take if the power target limit is not achieved within the specified power policy grace period. You can choose to specify one of the following actions: • **None**. If you enable this option and the power target limit is not achieved, Oracle ILOM will display a status error message to notify you that Oracle ILOM is unable to achieve the power capping limit specified. *or* • **Hard Power Off**. If you enable this option and the power target limit is not achieved, Oracle ILOM takes the following actions: * Displays a status error message. * Initiates a hard-power-off of the server. **Note -** The default option for Violation Actions is **None.**

Note – For best power capping performance, the default values are recommended for all advanced server power limit properties.

---

4. **To apply the power limit property changes, click Save.**

Configuring Power Consumption Threshold Notifications (Web)

Description	Links	Platform Feature Support
View or configure power consumption notification thresholds from Oracle ILOM	• "View and Configure Notification Thresholds Using the Web Interface" on page 114	• x86 servers • SPARC servers • CMM

▼ View and Configure Notification Thresholds Using the Web Interface

Before You Begin

- Review the power monitoring terminology defined in the *Oracle ILOM 3.0 Daily Management Concepts Guide.*
- The platform server or CMM must be running Oracle ILOM firmware version 3.0.4 or later.
- You must have the Admin (a) role enabled in Oracle ILOM to modify the power consumption configuration variables.

1. **Log in to the Oracle ILOM SP or CMM web interface.**

2. **In the web interface page, click Power Management --> Consumption.**

   The Power Consumption page appears.

3. **In the Power Consumption page, perform the following steps:**

   a. **Click (check) the Enabled check box for Notification Threshold (1) or (2).**

   b. **Based on your system requirements, type a notification threshold wattage value in the Watts text box.**

   c. **To apply these changes, click Save.**

Monitoring and Configuring Component Power Allocation Distributions (Web)

Description	Links	Platform Feature Support
Review the prerequisites for configuring the component power allocations	• "Requirements for Power Allocation Distributions (Web)" on page 115	• x86 servers • SPARC servers • CMM
View component allocation metrics for server or CMM	• "View Server Component Power Allocations (Web)" on page 116 • "View CMM Component Power Allocations" on page 120	• x86 servers • SPARC servers • CMM
Configure permitted power for blade slots in chassis	• "Configure Permitted Power for Blade Slots in CMM as of Oracle ILOM 3.0.6" on page 123 • "Configure Grant Limit for Blade Slots in CMM as of Oracle ILOM 3.0.10" on page 124	• CMM

Requirements for Power Allocation Distributions (Web)

- Review the power monitoring terminology defined in the *Oracle ILOM 3.0 Daily Management Concepts Guide.*
- Review the conceptual information about Component Allocation Power Distribution in the *Oracle ILOM 3.0 Daily Management Concepts Guide.*
- The platform server or the CMM must be running Oracle ILOM firmware version 3.0.6 or later. Where noted, some procedures described in this section require the server SP or CMM to be running Oracle ILOM firmware version 3.0.10 or later.
- You must have the admin (a) role enabled in Oracle ILOM to modify power consumption or allocation configuration property values.

Note – As of Oracle ILOM firmware version 3.0.8, the server SP Power Management --> Distribution tab was renamed to Allocation. As of Oracle ILOM firmware version 3.0.10, the CMM Power Management --> Distribution tab was renamed to Allocation.

▼ View Server Component Power Allocations (Web)

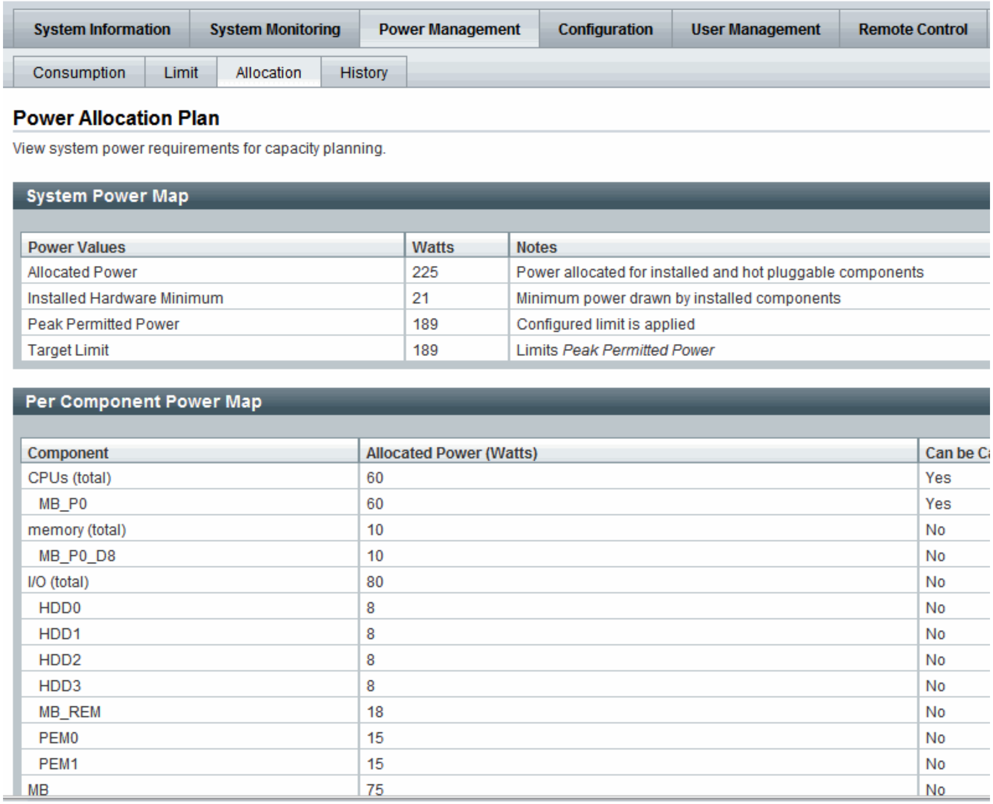
Before You Begin

- Review the "Requirements for Power Allocation Distributions (Web)" on page 115.

To review the server component power allocations, follow these steps:

1. **Log in to the Oracle ILOM SP web interface.**
2. **In the web interface, do one of the following:**
   - If the server is running ILOM firmware version 3.0.6, click Power Management --> Distribution.
   - If the server is running Oracle ILOM firmware version 3.0.8 or later, click Power Management --> Allocation.

   The Power Distribution or Power Allocation Plan page appears.



Power Allocation Plan

View system power requirements for capacity planning.

System Power Map

Power Values	Watts	Notes
Allocated Power	225	Power allocated for installed and hot pluggable components
Installed Hardware Minimum	21	Minimum power drawn by installed components
Peak Permitted Power	189	Configured limit is applied
Target Limit	189	Limits *Peak Permitted Power*

Per Component Power Map

Component	Allocated Power (Watts)	Can be Ca
CPUs (total)	60	Yes
MB_P0	60	Yes
memory (total)	10	No
MB_P0_D8	10	No
I/O (total)	80	No
HDD0	8	No
HDD1	8	No
HDD2	8	No
HDD3	8	No
MB_REM	18	No
PEM0	15	No
PEM1	15	No
MB	75	No

3. **In the allocation power tables, view the following system power requirements for power capacity planning:**

   - **System Power Map** – This table reflects the total power allocated value in wattage for the following system power properties: Allocated Power, Installed Hardware Minimum, Peak Permitted Power, and Target Limit.
   - **Per Component Power Map** – This table reflects the allocated power wattage value for each server component category (for example, memory) and each server component (for example ME_PO_D0). It also identifies whether the allocated power value can be capped.

▼ Configure Server Power Limit Properties as of Oracle ILOM 3.0.8 (Web)

Before You Begin

- Review the “Requirements for Power Allocation Distributions (Web)” on page 115.

To set power limit properties for servers running Oracle ILOM firmware version 3.0.8 or later, follow these steps:

1. **Log in to the Oracle ILOM SP web interface.**

2. **In the Oracle ILOM web interface, click Power Management --> Limit tabs.**

Note – The Power Management --> Distribution tab was renamed to Limit as of Oracle ILOM 3.0.8.

   The Power Limit page appears.

3. **In the Power Limit page, view or modify any of the following power limit properties.**

Power Limit Property	Description
Power Limiting	Enable this property to enable the power limit configuration.

Power Limit Property	Description
Target Limit	Set a target limit in watts or as a percentage. This value should reflect a range between the installed hardware minimum power and the allocated power. **Note -** You can view the installed hardware minimum power value and the allocated power value on the power management --> allocation tab.
Policy	The Policy property enables you to configure the power capping policy. In the policy property, specify which of the following types of power capping you want to apply: • **Soft - Only cap if actual power exceeds target limit**. If you enabled the soft cap option, you can configure the grace period for capping actual power to within the target limit. - **System Default**. This option, when selected, applies the default optimum grace period property values that is specified by the platform server. *or* - **Custom**. This option, when selected, applies the grace period property value specified by the user. • **Hard - Fixed cap keeps peak permitted power under target limit**. If you enable the hard cap option, power capping is permanently applied without a grace period.
Violation Actions	The Violation Actions property enables you to specify the settings you want Oracle ILOM to take if the power target limit cannot be achieved within the set grace period. You can choose to specify one of the following actions: • **None**. If you enable this option and the power target limit is not achieved, Oracle ILOM will display a status error message to notify you that Oracle ILOM is unable to achieve the power capping limit specified. *or* • **Hard Power Off.** If this option is chosen and the power target limit is not achieved, Oracle ILOM takes the following actions: * Display a status error message. * Initiates a hard-power-off of the server. **Note -** The default option for Violation Actions is None.

Note – For best power capping performance, the default values are recommended for all advanced server power limit properties.

4. **To apply the power limit property changes, click Save.**

▼ View CMM Component Power Allocations

Before You Begin

- Review the "Requirements for Power Allocation Distributions (Web)" on page 115.

To view the CMM component power allocations in the Oracle ILOM web interface, follow these steps:

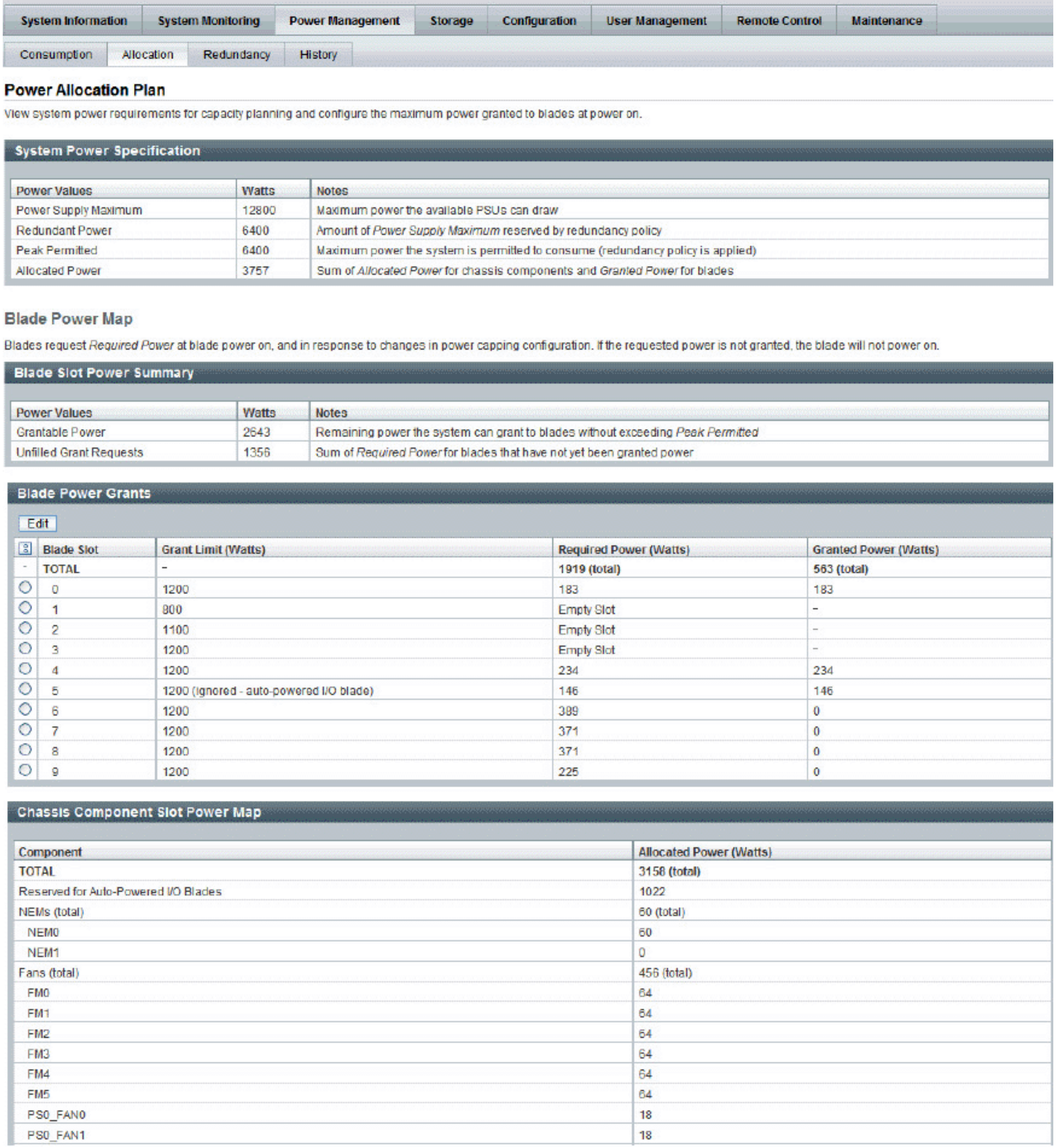
1. **Log in to the Oracle ILOM CMM web interface.**

2. **In the left pane of the CMM web interface page, select CMM then do one of the following:**

   - If the CMM is running Oracle ILOM firmware version 3.0.6 or later, select the Power Management --> Distribution tabs.
   - If the CMM is running Oracle ILOM firmware version 3.0.10 or later, select Power Management --> Allocation tabs.

Note – The CMM Power Management --> Distribution tab was renamed to Allocation in Oracle ILOM firmware version 3.0.10.

The CMM Power Allocation Plan page appears.



Power Allocation Plan

View system power requirements for capacity planning and configure the maximum power granted to blades at power on.

System Power Specification

Power Values	Watts	Notes
Power Supply Maximum	12800	Maximum power the available PSUs can draw
Redundant Power	6400	Amount of *Power Supply Maximum* reserved by redundancy policy
Peak Permitted	6400	Maximum power the system is permitted to consume (redundancy policy is applied)
Allocated Power	3757	Sum of *Allocated Power* for chassis components and *Granted Power* for blades

Blade Power Map

Blades request *Required Power* at blade power on, and in response to changes in power capping configuration. If the requested power is not granted, the blade will not power on.

Blade Slot Power Summary

Power Values	Watts	Notes
Grantable Power	2643	Remaining power the system can grant to blades without exceeding *Peak Permitted*
Unfilled Grant Requests	1356	Sum of *Required Power* for blades that have not yet been granted power

Blade Power Grants

	Blade Slot	Grant Limit (Watts)	Required Power (Watts)	Granted Power (Watts)
-	TOTAL	-	**1919 (total)**	**563 (total)**
○	0	1200	183	183
○	1	800	Empty Slot	-
○	2	1100	Empty Slot	-
○	3	1200	Empty Slot	-
○	4	1200	234	234
○	5	1200 (ignored - auto-powered I/O blade)	146	146
○	6	1200	389	0
○	7	1200	371	0
○	8	1200	371	0
○	9	1200	225	0

Chassis Component Slot Power Map

Component	Allocated Power (Watts)
TOTAL	**3158 (total)**
Reserved for Auto-Powered I/O Blades	1022
NEMs (total)	60 (total)
NEM0	60
NEM1	0
Fans (total)	456 (total)
FM0	64
FM1	64
FM2	64
FM3	64
FM4	64
FM5	64
PS0_FAN0	18
PS0_FAN1	18

3. **In the CMM Power Allocation page, view the power allocation values.**

- For Oracle ILOM firmware version 3.0.6 or later, the CMM power allocation values appear as follows:

Updated Property Name	Details
Allocated Power	Total power allocated value in wattage for all power-consuming CMM components in the system chassis.
Allocatable Power	Total remaining power (watts) available from CMM to allocate to blade slots.
Blade Slot Power Distribution	View power allocation values for: • **Allocated Power** – Total power (watts) allocated to the server module (blade) in this slot. The CMM always allocates enough power to handle an unengaged I/O server module, whether or not an I/O server module is present. • **Permitted Power** – Maximum power allocation permitted for a server module in this blade slot. **Note -** To modify the permitted power allocated to a server module slot, refer to the "Configure Permitted Power for Blade Slots in CMM as of Oracle ILOM 3.0.6" on page 123.
Component Power Distribution	View allocated power for each non-blade component in the system.

- For Oracle ILOM firmware version 3.0.10 or later, the CMM power allocation values appear as follows:

Updated Property Name	Details
Grantable Power (renamed property)	Allocatable Power in Oracle ILOM 3.0.6 was renamed to Grantable Power in Oracle ILOM firmware version 3.0.10. Grantable Power indicates the total remaining power (watts) available from the CMM to allocate to blade slots without exceeding grant limit.
Grant Limit (renamed property)	Permitted Power in Oracle ILOM 3.0.6 was renamed to Grant Limit in Oracle ILOM firmware version 3.0.10. Grant Limit represents the maximum power the system will grant to a blade slot. For instructions for setting the grant limit on a blade, see "Configure Permitted Power for Blade Slots in CMM as of Oracle ILOM 3.0.6" on page 123.
Granted Power (renamed property)	Allocated Power in Oracle ILOM 3.0.6 was renamed to Granted Power in Oracle ILOM firmware version 3.0.10. 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 all server power-consuming components.

▼ Configure Permitted Power for Blade Slots in CMM as of Oracle ILOM 3.0.6

Before You Begin

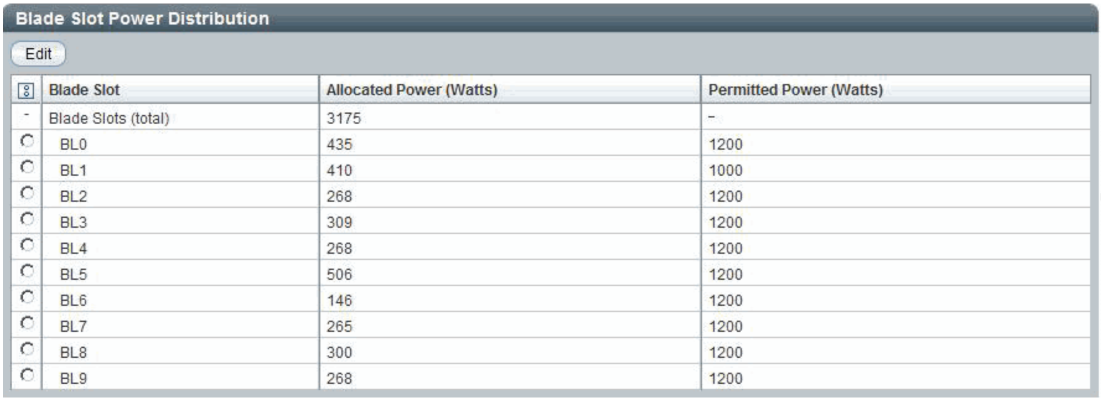
- Review the "Requirements for Power Allocation Distributions (Web)" on page 115.

To configure the permitted blade slot power in the Oracle ILOM web interface, follow these steps:

1. **Log in to the Oracle ILOM CMM web interface.**

2. **In the left pane of the web interface page, click CMM, and then click Power Management --> Distribution.**

3. **Scroll down to the Blade Slot Power Distribution table.**



Blade Slot Power Distribution

Edit

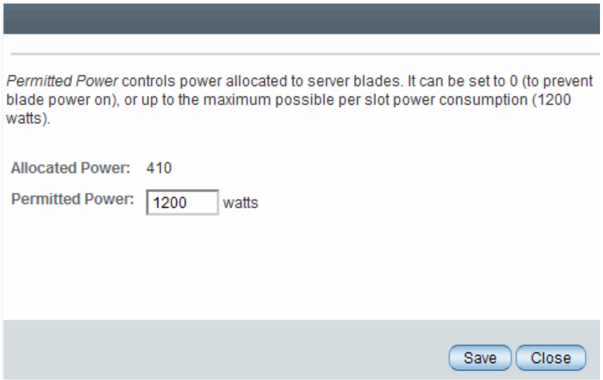
	Blade Slot	Allocated Power (Watts)	Permitted Power (Watts)
-	Blade Slots (total)	3175	-
○	BL0	435	1200
○	BL1	410	1000
○	BL2	268	1200
○	BL3	309	1200
○	BL4	268	1200
○	BL5	506	1200
○	BL6	146	1200
○	BL7	265	1200
○	BL8	300	1200
○	BL9	268	1200

4. **In the Blade Slot Power Distribution table, do the following.**

   a. **Enable the radio buttons next to the blade slots that you want to modify.**

   b. **Click Edit.**

   A dialog appears listing information about the Allocated and Permitted Power value.



Permitted Power controls power allocated to server blades. It can be set to 0 (to prevent blade power on), or up to the maximum possible per slot power consumption (1200 watts).

Allocated Power: 410

Permitted Power: 1200 watts

c. **In the dialog, modify the Permitted Power value, and then click Save.**

Note – To prevent server module from powering-on, you can set the Permitted Power value to `0`.

▼ Configure Grant Limit for Blade Slots in CMM as of Oracle ILOM 3.0.10

Before You Begin

- Review the "Requirements for Power Allocation Distributions (Web)" on page 115.

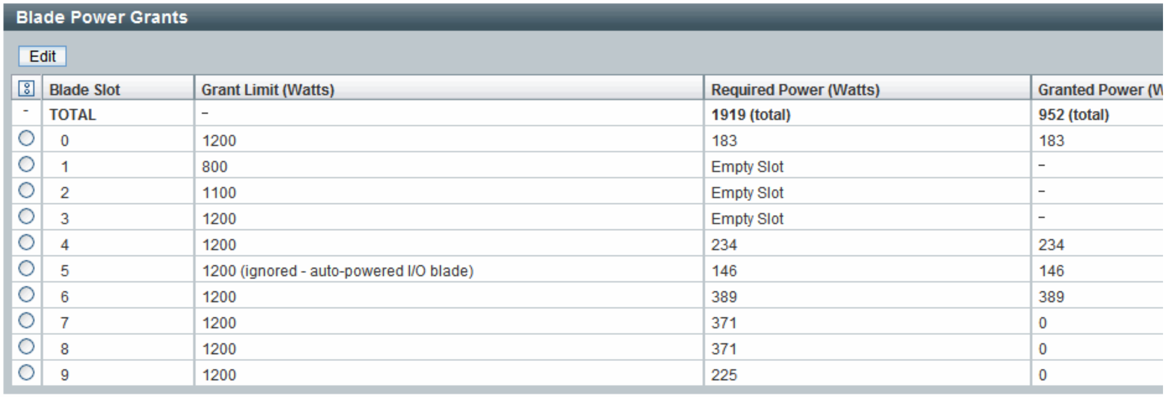
To configure the blade slot grant limit in the Oracle ILOM CMM web interface, follow these steps:

1. **Log in to the Oracle ILOM CMM web interface.**

2. **In the left pane of the web interface page, select CMM, and then in the right pane of the web interface page, click Power Management --> Allocation.**

   The CMM Power Allocation page appears.

3. **Scroll down to the Blade Slot Grants table.**



Blade Power Grants

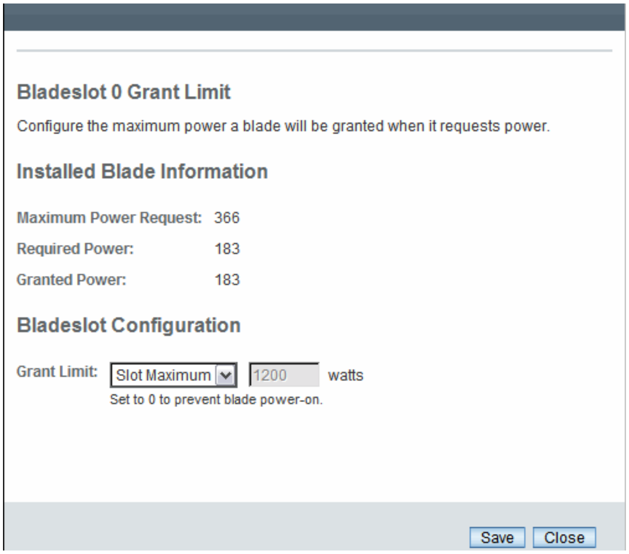
	Blade Slot	Grant Limit (Watts)	Required Power (Watts)	Granted Power (W
-	TOTAL	–	**1919 (total)**	**952 (total)**
○	0	1200	183	183
○	1	800	Empty Slot	–
○	2	1100	Empty Slot	–
○	3	1200	Empty Slot	–
○	4	1200	234	234
○	5	1200 (ignored - auto-powered I/O blade)	146	146
○	6	1200	389	389
○	7	1200	371	0
○	8	1200	371	0
○	9	1200	225	0

4. **In the Blade Slot Grants table, do the following.**

   a. **Enable the radio buttons next to the blade slot that you want to modify.**

   b. **Click Edit.**

   A dialog appears listing power configuration information for the blade.



Bladeslot 0 Grant Limit

Configure the maximum power a blade will be granted when it requests power.

Installed Blade Information

Maximum Power Request: 366

Required Power: 183

Granted Power: 183

Bladeslot Configuration

Grant Limit: Slot Maximum 1200 watts

Set to 0 to prevent blade power-on.

   c. **In the Grant Limit list box, choose to use the default slot maximum grant limit (1200 watts), or click Custom and type a power grant value and click Save.**

Note – To prevent the blade from powering-on, you can set the Grant Limit value to `0`.

Configuring Server Power Limit Properties (Web)

Description	Links	Feature Platform Support
Manage server power limit properties from Oracle ILOM	• "Configure Server Power Limit Properties (Web)" on page 126	• x86 Server SP • SPARC Server

▼ Configure Server Power Limit Properties (Web)

Before You Begin

- Review the power monitoring terminology defined in the *Oracle ILOM 3.0 Daily Management Concepts Guide.*
- Review the conceptual information about server power limit (or server power budget) in the *Oracle ILOM 3.0 Daily Management Concepts Guide.*
- The platform server must be running Oracle ILOM firmware version 3.0.6 or later to configure the server power limit properties.
- You must have the admin (a) role enabled in Oracle ILOM to modify power management configuration property values.

Note – As of Oracle ILOM firmware version 3.0.8, the server SP Power Management --> Budget tab was renamed to Limit.

---

1. **Log in to the Oracle ILOM SP web interface.**
2. **In the Oracle ILOM web interface, do one of the following:**
   - If the platform server is running Oracle ILOM firmware version 3.0.6, click Power Management --> Budget.
   - If the platform server is running Oracle ILOM firmware version 3.0.8 or later, click Power Management --> Limit.
3. **In the Power Limit page, view or modify the power limit properties described in the following table.**

Power Limit Property	Description
Power Limiting	Enable this property to enable the power limit configuration. **Note -** Power limiting was previously named Activation State on the Budget tab in Oracle ILOM 3.0.6.
Target Limit	Set a target limit in watts or as a percentage. This value should reflect a range between the Installed Hardware Minimum Power and the Allocated Power. **Note -** In Oracle ILOM firmware version 3.0.6, the Budget tab option for Target Limit was previously named Power Limit. **Note -** You can view the installed hardware minimum power value and the allocated power value on the Power Management --> Allocation tab.

Power Limit Property	Description
Status Error Message	The status error message read-only property only appears on the Limit page when Oracle ILOM fails to achieve the power limit that was configured. **Note -** The status error message read-only property was previously named Status on the Budget tab in Oracle ILOM firmware version 3.0.6.
Policy	The Policy property enables you to configure the power capping policy. In the Policy property, specify which of the following types of power capping you want to apply: • **Soft - Only cap if actual power exceeds Target Limit**. If you enabled the soft cap option, you can configure the grace period for capping actual power to within the target limit. **- System Default**. This option, when selected, applies the default optimum grace period property values that is specified by the platform server. *or* **- Custom**. his option, when selected, applies the grace period property value specified by the user. • **Hard - Fixed cap keeps Peak Permitted power under Target Limit**. If you enable the hard cap option, power capping is permanently applied without a grace period. **Note -** The Policy was previously named Time Limit on the Budget tab in Oracle ILOM firmware version 3.0.6.
Violation Actions	The Violation Actions property enables you to specify the settings you want Oracle ILOM to take if the power target limit is not achieved within the set grace period. You can choose to specify one of the following actions: • **None**. If you enable this option and the power target limit is not achieved, Oracle ILOM will display a status error message to notify you that Oracle ILOM is unable to achieve the power capping limit specified. *or* • **Hard-Power Off**. If you enable this option and the power target limit is not achieved, Oracle ILOM takes the following actions: * Display a status error message. * Initiates a hard-power-off of the server. **Note -** The default option for Violation Actions is None.

Note – For best power capping performance, the default values are recommended for all advanced server power limit properties.

4. **To apply the power limit property changes, click Save.**

Monitoring or Configuring CMM Power Supply Redundancy (Web)

Description	Links	Feature Platform Support
Manage CMM power supply redundancy properties from Oracle ILOM	• "View or Configure CMM Power Supply Redundancy Properties (Web)" on page 129	• CMM

▼ View or Configure CMM Power Supply Redundancy Properties (Web)

Before You Begin

- Review the power monitoring terminology defined in the *Oracle ILOM 3.0 Daily Management Concepts Guide.*
- Review the conceptual information about power supply redundancy for CMM systems in the *Oracle ILOM 3.0 Daily Management Concepts Guide.*
- The server must be running Oracle ILOM firmware version 3.0.6 or later to configure the CMM power supply redundancy properties.
- You must have the admin (a) role enabled in Oracle ILOM to modify power management configuration property values.

To view or configure the CMM power supply redundancy property values, follow these steps:

1. **Log in to the Oracle ILOM CMM web interface.**
2. **In the left pane of the CMM web interface, click CMM, and then in the right pane of the web interface page, click Power Management --> Redundancy.**

   The Power Management Redundancy page appears.
3. **In the Redundancy page, view or configure the properties.:**
   - **Power Supply Redundancy Policy** – Select the number of power supplies to allocate for redundancy.

- **None** – To reserve no power supplies.
- **N+N** – To reserve half of the power supplies.

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 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.

- **Redundant Power** – This value is provided by the system. It represents the available power that is not allocated.

4. **To apply the changes made, click Save.**

Managing Remote Hosts Redirection and Securing the Oracle ILOM Remote Console (Web)

Description	Links
Details for locating instructions for using the Oracle ILOM Remote Console.	• “Web Procedures for Redirecting Remote Host KVMS” on page 131

Related Information

- *Oracle ILOM 3.0 Remote Redirection Consoles*, remote host management Options
- *Oracle ILOM 3.0 Remote Redirection Consoles*, manage remote hosts storage Redirection
- *Oracle ILOM 3.0 Remote Redirection Consoles*, secure the Oracle ILOM Remote Console

Web Procedures for Redirecting Remote Host KVMS

The Oracle ILOM Remote Console, available from the web interface, provides remote redirection for the following devices: keyboard, video, mouse, and storage devices. To use the Oracle ILOM Remote Console, you must have the Console (c) role enabled in Oracle ILOM.

As of ILOM 3.0.16, the information describing how to use Oracle ILOM Remote Console was moved to the *Oracle ILOM 3.0 Remote Redirection Consoles CLI and Web Guide*. For detailed instructions for using the Oracle ILOM Remote Console, refer to these topics:

- *Oracle ILOM 3.0 Remote Redirection Consoles*, initial set up tasks to support the Oracle ILOM Remote Console
- *Oracle ILOM 3.0 Remote Redirection Consoles*, redirecting devices using the Oracle ILOM Remote Console
- *Oracle ILOM 3.0 Remote Redirection Consoles*, securing the Oracle ILOM Remote Console.

Managing Remote Hosts Power States (Web)

Description	Links
Control the power state of a remote server module or CMM	• "Controlling Power States From Remote Server SP or CMM (Web)" on page 134
Control x86 Host boot device settings	• "Managing Host Control of Boot Device on x86 Systems (Web)" on page 135

Related Information

- *Oracle ILOM 3.0 Daily Management Concepts*, remote host management options
- *Oracle ILOM 3.0 Daily Management CLI Procedures*, manage remote hosts power states
- *Oracle ILOM 3.0 Daily Management CLI Procedures*, manage BIOS boot device
- *Oracle ILOM 3.0 Daily Management CLI Procedures*, manage host server console

Controlling Power States From Remote Server SP or CMM (Web)

Description	Links	Platform Feature Support
Control the power state of the remote host server	• "Control Power State of Remote Host Server Using Server SP (Web)" on page 134	• x86 system server SP • SPARC system server SP
Control the power state of the remote CMM	• "Control Power State of Remote Chassis Using the CMM Web Interface" on page 135	• CMM

▼ Control Power State of Remote Host Server Using Server SP (Web)

Before You Begin

- To control the power state of the remote host server, you need the Admin (a) role enabled.

To control the power state of a remote host server, follow these steps:

1. **Log in to the Oracle ILOM SP web interface.**

2. **Click the Remote Power Control tab.**

   The Server Power Control page appears.

3. **From the Server Power Control page, you can remotely control the power state of a host server by selecting one of the following options from the Action menu:**
   - **Reset** – This option immediately reboots the remote host server.
   - **Immediate Power Off** – This option immediately turns off the power on the remote host server.
   - **Graceful Shutdown and Power Off** – This option shuts down the OS gracefully prior to powering off the remote host server.
   - **Power On** (default) – This option turns on full power to the remote host server.
   - **Power Cycle** – This option immediately turns off the power on the remote host server, then applies full power to the remote host server.

▼ Control Power State of Remote Chassis Using the CMM Web Interface

Before You Begin

- To control the power state of the remote chassis and its system components, you need the admin (a) role enabled.

To control the power state of the chassis and its system components, follow these steps:

1. **Log in to the Oracle ILOM CMM web interface.**
2. **Click the Remote Power Control tab.**

   The Server Power Control page appears.
3. **From the CMM Remote Power Control page, you can remotely control the power state of the chassis and its system components by selecting the radio button next to /CH (Chassis) or /CH/BL# (individual blade slot #) then selecting one of the following options from the Action menu:**
   - **Immediate Power Off** – This option immediately turns off the power to the chassis components, including the blades.
   - **Graceful Shutdown and Power Off** – This option attempts to bring the OS down gracefully on the blades, then cuts power to the system components.
   - **Power On** – This option gives full power to the chassis and blades, subject to system policies.
   - **Power Cycle** – This option powers off the blade, then automatically powers the system back on (not applicable to /CH).

Managing Host Control of Boot Device on x86 Systems (Web)

Description	Link	Platform Feature Support
Review the prerequisites	• "Requirements for Host Boot Device (Web)" on page 136	• x86 system server SP
Override host boot device order in BIOS	• "Configure Host Boot Device (Web)" on page 136	

Requirements for Host Boot Device (Web)

- To modify the host boot device configuration property value, you must have the Reset and Host Control (r) role enabled in Oracle ILOM.
- The host control BIOS boot device feature in Oracle ILOM is supported on x86 system SPs. This feature is not supported on the CMM or on SPARC system SPs. For information about Oracle ILOM Host Control boot options on SPARC systems, review to the platform server Oracle ILOM supplement guide or platform administration guide.

▼ Configure Host Boot Device (Web)

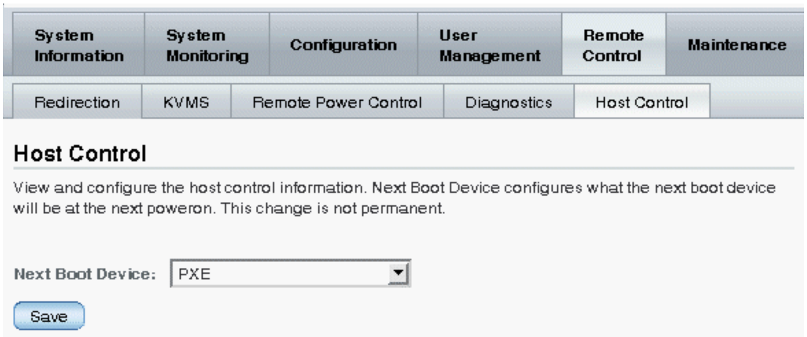
Before You Begin

- Review the "Requirements for Host Boot Device (Web)" on page 136

To override the BIOS boot device setting from Oracle ILOM web interface, follow these steps:.

1. **Log in to the Oracle ILOM SP web interface.**
2. **Click Remote Control --> Host Control.**

   The Host Control page appears.



Host Control

View and configure the host control information. Next Boot Device configures what the next boot device will be at the next poweron. This change is not permanent.

Next Boot Device: PXE

3. **In the Host Control page, click the Next Boot Device list box and specify a boot device option.**

   Possible boot device options available:

   - **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.

4. **To apply your changes, click Save.**

Managing TPM and LDom States on SPARC Servers (Web)

Description	Links
Control the TPM state on a SPARC server	• "Controlling the TPM State on SPARC Servers (Web)" on page 139
Manage Logical Domain (LDom) configurations on SPARC servers	• "Managing LDom Configurations on SPARC Servers (Web)" on page 141

Related Information

- *Oracle ILOM 3.0 Daily Management Concepts*, remote host management options
- *Oracle ILOM 3.0 Daily Management CLI Procedures*, manage TPM and LDom states on SPARC servers

Controlling the TPM State on SPARC Servers (Web)

Description	Link	Platform Feature Support
Control the TPM state on a SPARC server	• "Control TPM State on a SPARC Server (Web)" on page 139	• SPARC system server SP

▼ Control TPM State on a SPARC Server (Web)

Before You Begin

- The TPM feature in Oracle ILOM is available for SPARC servers only.
- The SPARC server should be running a version of Oracle Solaris that supports TPM.

  For more information about configuring TPM support in Oracle Solaris, refer to the Oracle Solaris documentation or the platform documentation shipped with your server.
- You must be using Oracle ILOM 3.0.8 or a later version on the SPARC server SP.
- You need to have the Reset and Host Control (`r`) role enabled in Oracle ILOM to modify the TPM settings.

To control the TPM state on a SPARC server, following these steps:

1. **Log in to the Oracle ILOM SP web interface.**
2. **Click the Remote Control --> TPM tab.**

   The TPM Settings page appears.
3. **In the TPM Settings page, do one of the following:**
   - To enable the TPM state and activate this enabled state on the SPARC server the next time it is powered on, select **True** for the following TPM settings:
     - **Enable** – Click (check) the Enable True check box to enable the TPM state on the SPARC server.
     - **Activate** – Click (check) the Activate True check box to activate the configuration change on the SPARC server the next time the server powers on.

   or
   - To purge (disable) an enabled TPM state on the SPARC server the next time the server powers on, select **True** for following three TPM settings:
     - **Enable** – Clear the Enable True check box to disable the TPM state on the SPARC.
     - **Activate** – Click (check) the Activate True check box to activate the configuration change on the SPARC server.
     - **Forceclear** – Click (check) the Forceclear True check box to purge the enabled TPM state from the SPARC server the next time the server powers on.

Managing LDom Configurations on SPARC Servers (Web)

Descriptions	Links	Platform Feature Support
Review the prerequisites	• "Requirements for SPARC LDom Configurations (Web)" on page 141	• SPARC system server SP
View and manage Oracle ILOM settings for stored LDom configurations	• "View Stored LDom Configurations on SPARC T3 Series Server (Web)" on page 142 • "Configure Host Power to Stored LDom Configurations (Web)" on page 143 • "Specify Host Power to a Stored LDom Configuration (Web)" on page 143	

Requirements for SPARC LDom Configurations (Web)

To view and manage the Oracle ILOM settings for stored LDom configurations, the following requirements must be met:

- You must access Oracle ILOM on a SPARC server that has the appropriate Oracle ILOM point release firmware installed (see Note below).

Note – Oracle ILOM firmware version 3.0.12 or later is required to view the LDom targets and properties from a SPARC T3 Series server. Oracle ILOM firmware version 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*.
- You must have the Remote Host Reset and Host Control (`r`) role enabled in Oracle ILOM to modify the LDom host domains property values.

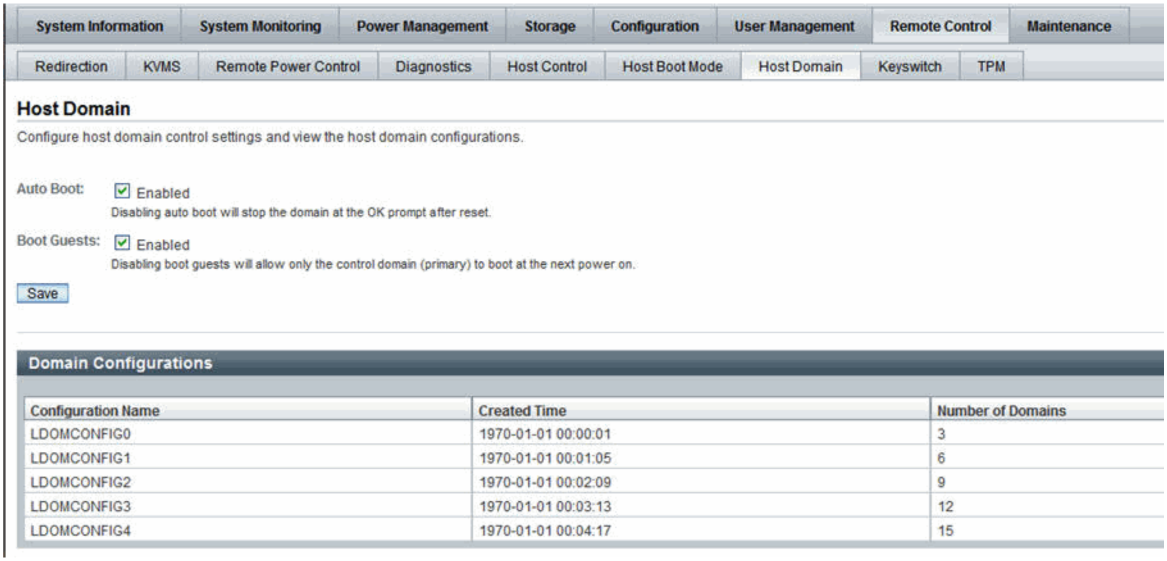
▼ View Stored LDom Configurations on SPARC T3 Series Server (Web)

Before You Begin

- Review the "Requirements for SPARC LDom Configurations (Web)" on page 141

To view LDom configurations on a SPARC T3 series server, follow these steps:

1. **Log in to the Oracle ILOM web interface on a SPARC T3 Series Server.**
2. **In the web interface, click Remote Host --> Host Domains.**
3. **In the Domain Configurations table, you can view a list of LDom Configurations currently saved in LDom Manager.**



Host Domain

Configure host domain control settings and view the host domain configurations.

Auto Boot: ☑ Enabled
Disabling auto boot will stop the domain at the OK prompt after reset.

Boot Guests: ☑ Enabled
Disabling boot guests will allow only the control domain (primary) to boot at the next power on.

Domain Configurations

Configuration Name	Created Time	Number of Domains
LDOMCONFIG0	1970-01-01 00:00:01	3
LDOMCONFIG1	1970-01-01 00:01:05	6
LDOMCONFIG2	1970-01-01 00:02:09	9
LDOMCONFIG3	1970-01-01 00:03:13	12
LDOMCONFIG4	1970-01-01 00:04:17	15

4. **To commit the changes made on the Host Domain page, click Save.**

▼ Configure Host Power to Stored LDom Configurations (Web)

Before You Begin

- Review the "Requirements for SPARC LDom Configurations (Web)" on page 141.

To configure host power to the stored LDom configurations, follow these steps:

1. **Log in to the Oracle ILOM web interface on a SPARC server.**
2. **In the web interface, click Remote Host --> Host Domains.**
3. **In the Host Domain page, enable or disable the Auto Boot or Boot Guest check boxes.**

   By default, the Auto Boot check box for the host control domain and guest domains are set to `enabled` (boots when server is powered-on or reset).

   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. Disabling the boot guests property value for the guest domains will prevent the guest domains from booting after the next power-on or reset.

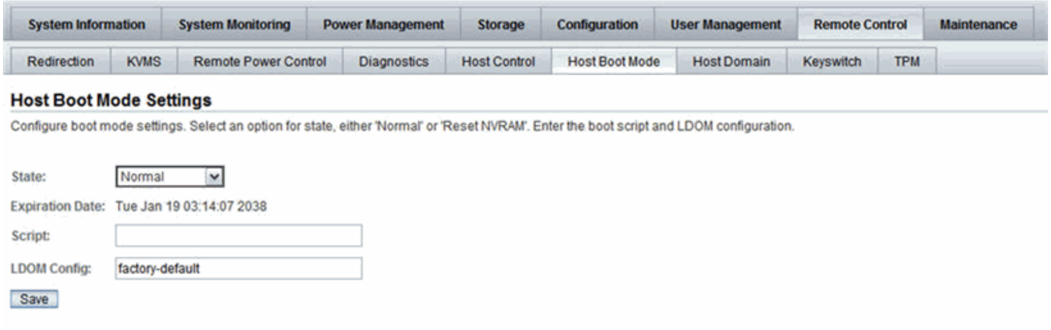
▼ Specify Host Power to a Stored LDom Configuration (Web)

Before You Begin

- Review the "Requirements for SPARC LDom Configurations (Web)" on page 141.

To specify host power to a stored LDom configuration, follow these steps:

1. **Log in to the Oracle ILOM web interface on a SPARC server.**
2. **In the web interface, click Remote Host --> Host Boot Mode.**



Host Boot Mode Settings

Configure boot mode settings. Select an option for state, either 'Normal' or 'Reset NVRAM'. Enter the boot script and LDOM configuration.

State: Normal

Expiration Date: Tue Jan 19 03:14:07 2038

Script:

LDOM Config: factory-default

3. **In the Host Boot Mode Settings page, specify the following information to override the default method the server uses to boot.**

Field	Instructions and Description
State	In the State list box, select one of the following options: • **Normal**. At next reset, this option will retain the current NVRAM variable settings. • **Reset NVRAM**. At next reset, this option will return all OpenBoot variables to default settings. The State dictates the boot mode at reset. **Note -** The Reset NVRAM value will return to normal after the next server reset or 10 minutes. The Config and Script properties do not expire and will be cleared upon the next server reset or manually by leaving the fields blank.
Script	Specify a boot script. The script controls the host server OpenBoot PROM firmware method of booting. It does not affect the current `/HOST/bootmode` setting.
LDOM Config	Specify a saved LDom configuration file name.

4. **To commit the changes made on the Host Boot Mode Settings page, click Save.**

Diagnosing IPv4 or IPv6 Oracle ILOM Connection Issues

The following topic provides solutions to help resolve common problems when accessing Oracle ILOM using IPv6.

- "Diagnosing Oracle ILOM Connection Issues" on page 145

Diagnosing Oracle ILOM Connection Issues

If you are experiencing difficulties with connecting to Oracle ILOM when using IPv6, use the information provided in TABLE: Common IPv6 Connection Problems and Suggested Resolutions on page 145 to help resolve common problems when accessing Oracle ILOM using IPv6.

TABLE: Common IPv6 Connection Problems and Suggested Resolutions

IPv6 Common Connection Problems	Suggested Resolution
Unable to access the Oracle 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`

TABLE: Common IPv6 Connection Problems and Suggested Resolutions *(Continued)*

IPv6 Common Connection Problems	Suggested Resolution
Unable to access Oracle ILOM using IPv6 from a network client.	If on a separate subnet, try the following: • Verify that Oracle 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 Oracle ILOM web interface or under the `/SP/network/ipv6` target in the Oracle ILOM CLI. • Run `ping6` in a restricted shell. • Run `traceroute` in a restricted shell.
Unable to access Oracle 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 Oracle 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 Oracle ILOM web interface or under the `/SP/network/ipv6` target.
Unable to access Oracle ILOM using IPv4 from a network client.	Ensure that the setting for `State` is enabled on the Network Settings page in the Oracle ILOM web interface or under the `/SP/network` target in the Oracle ILOM CLI.

Manual Host OS Configuration Guidelines for Local Interconnect Interface

The following topic provides guidelines for manually configuring a non-routable IPv4 address for the host OS connection point on the Local Interconnect Interface.

Configuring Internal USB Ethernet Device on Host OS

If you chose to manually configure a non-routable IPv4 address for the Oracle 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 the following table. For additional information about configuring IP addresses on the host operating system, consult the vendor operating system documentation.

Note – Oracle ILOM will present the internal USB Ethernet device installed on your server as an USB Ethernet interface to the host operating system.

TABLE: 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*. 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 ().

Linux	Most supported Linux operating system installations on an Oracle Sun platform 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: General Guidelines for Configuring Internal USB Ethernet Device on Host OS *(Continued)*

Operating System	General Guidelines

Oracle Solaris	Most Oracle 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 Oracle Solaris-specific OS driver for the Ethernet interface, see the *Oracle Server Hardware Management Pack User's Guide*.
	Typically, the internal USB Ethernet device is automatically discovered by the Oracle 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 Oracle Solaris operating system.
	After the Oracle 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 Oracle Solaris host or the SP internal USB Ethernet device.
	`ping` *<IPv4 address of Oracle 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 Oracle 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 Oracle Solaris Operating System, refer to the Oracle 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, refer to the *Oracle Server Hardware Management Pack User's Guide*.

Index